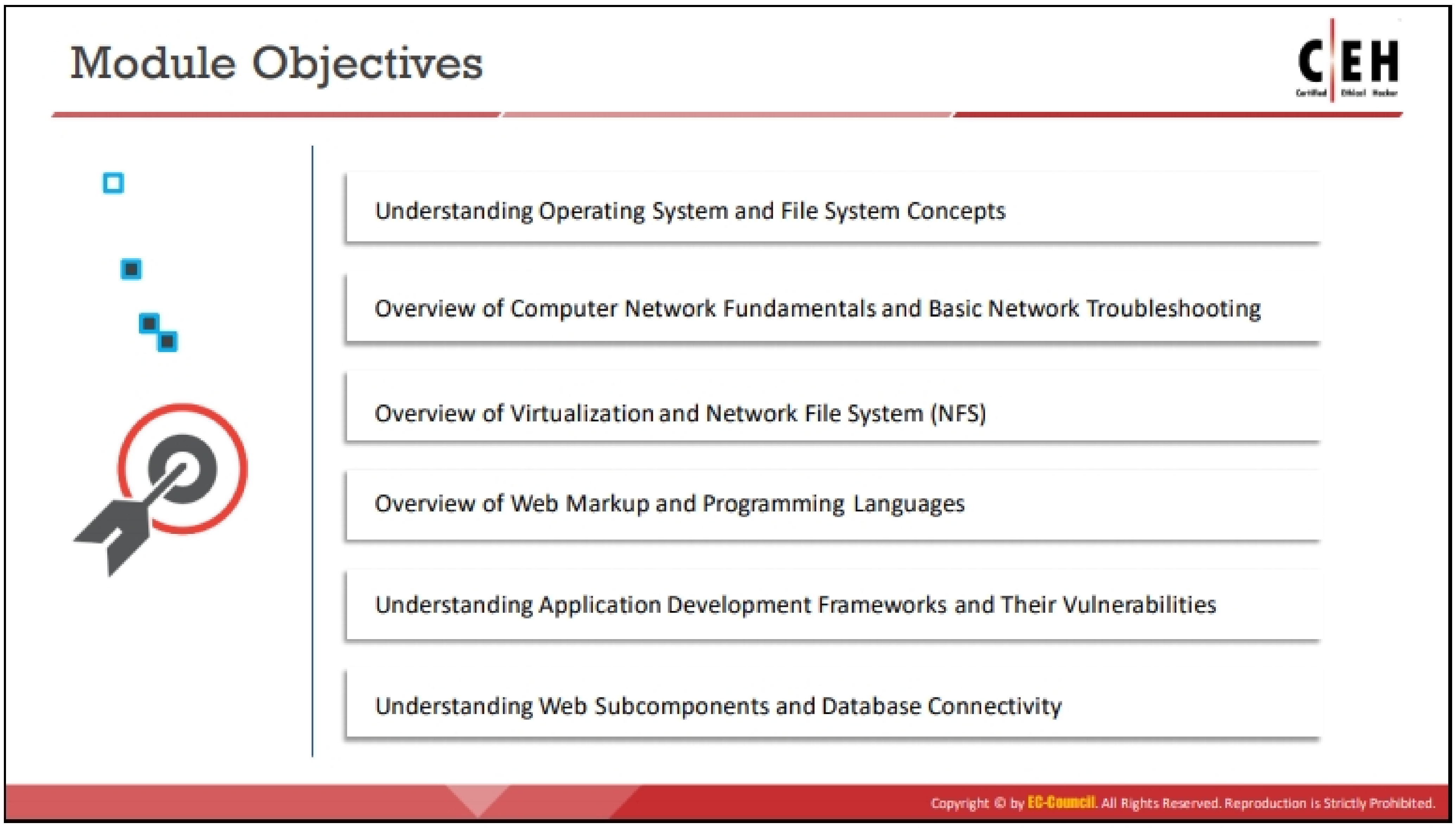
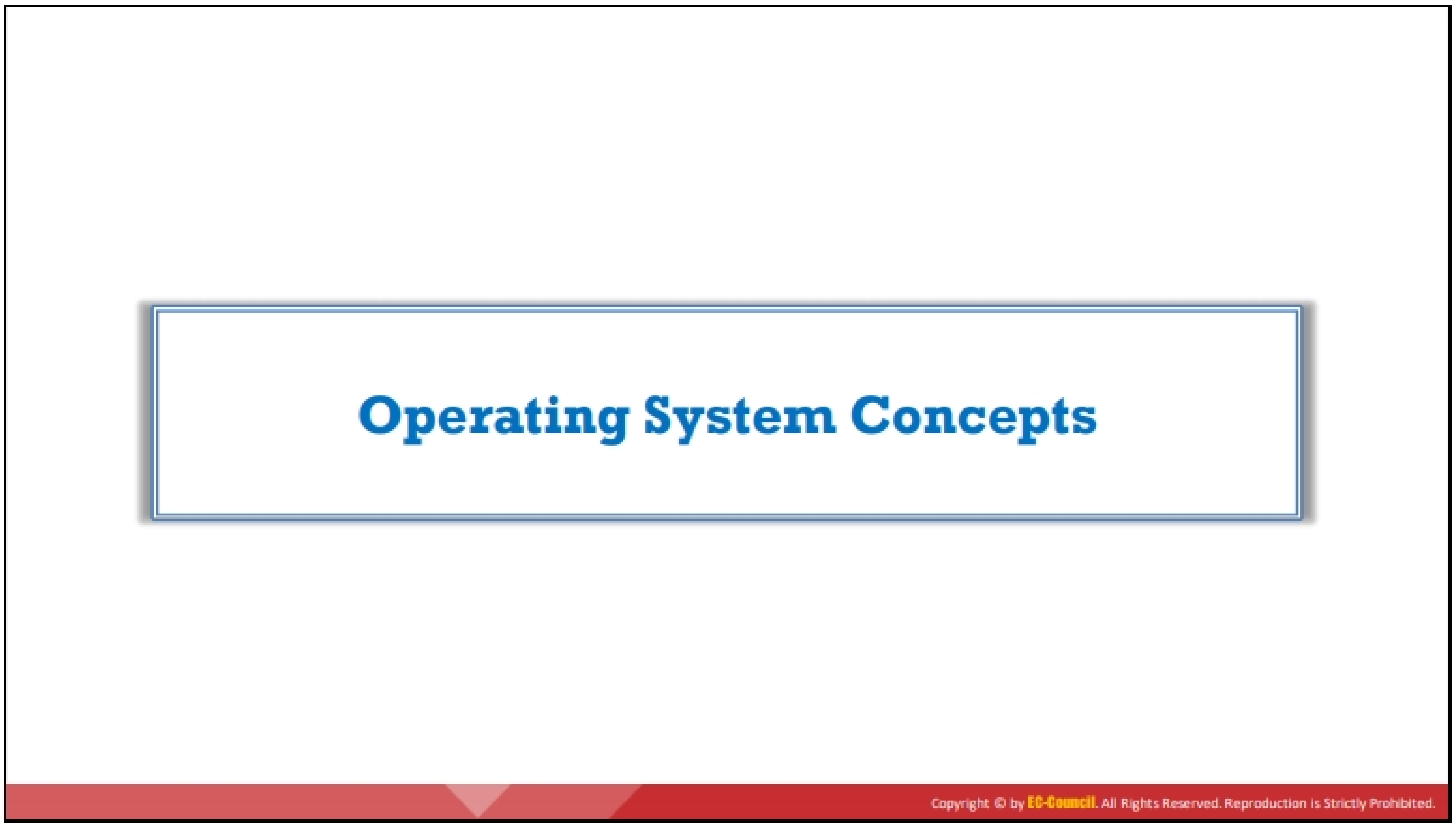
C|EH™
Certified Ethical Hacker

Appendix A:
Ethical Hacking Essential Concepts - I



Module Objectives

- Understanding Operating System and File System Concepts
- Overview of Computer Network Fundamentals and Basic Network Troubleshooting
- Overview of Virtualization and Network File System (NFS)
- Overview of Web Markup and Programming Languages
- Understanding Application Development Frameworks and Their Vulnerabilities
- Understanding Web Subcomponents and Database Connectivity



Operating System Concepts

Notes: ____

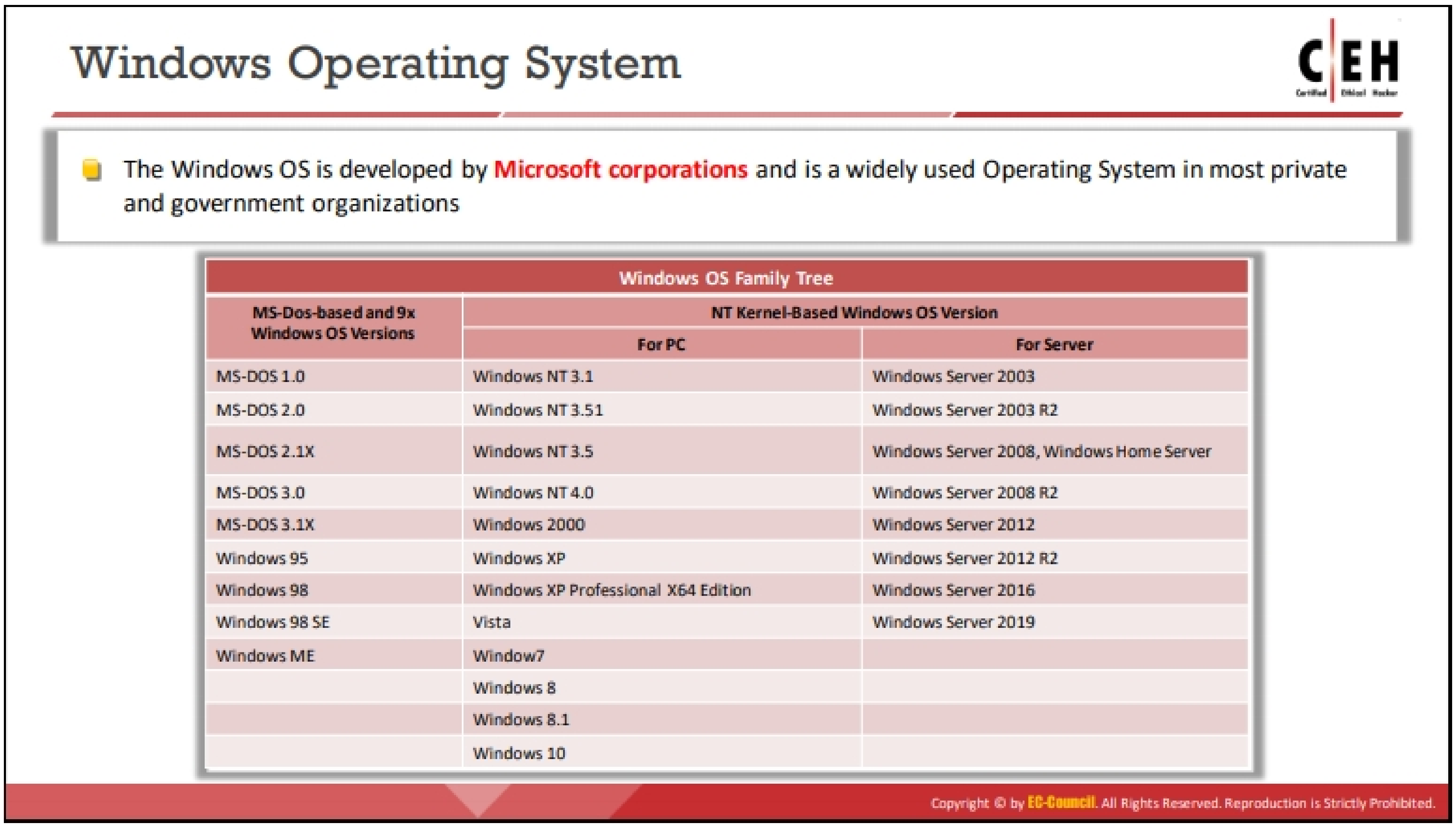
____

____

____

____

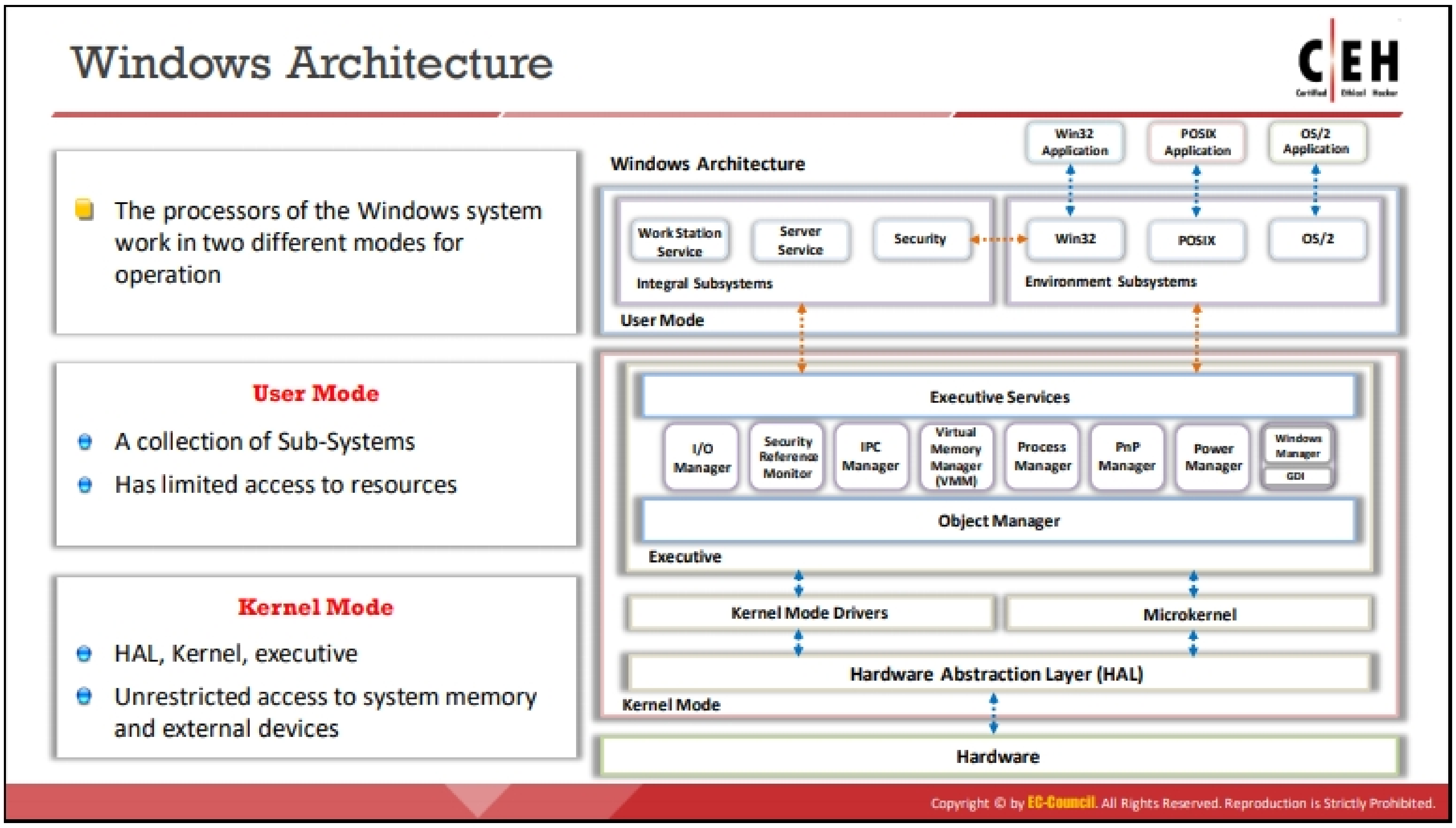
____



Windows Operating System

- The Windows OS is developed by **Microsoft corporations** and is a widely used Operating System in most private and government organizations

Windows OS Family Tree		
MS-Dos-based and 9x Windows OS Versions	**NT Kernel-Based Windows OS Version**	
	For PC	**For Server**
MS-DOS 1.0	Windows NT 3.1	Windows Server 2003
MS-DOS 2.0	Windows NT 3.51	Windows Server 2003 R2
MS-DOS 2.1X	Windows NT 3.5	Windows Server 2008, Windows Home Server
MS-DOS 3.0	Windows NT 4.0	Windows Server 2008 R2
MS-DOS 3.1X	Windows 2000	Windows Server 2012
Windows 95	Windows XP	Windows Server 2012 R2
Windows 98	Windows XP Professional X64 Edition	Windows Server 2016
Windows 98 SE	Vista	Windows Server 2019
Windows ME	Window7	
	Windows 8	
	Windows 8.1	
	Windows 10	



Windows Architecture

- The processors of the Windows system work in two different modes for operation

User Mode

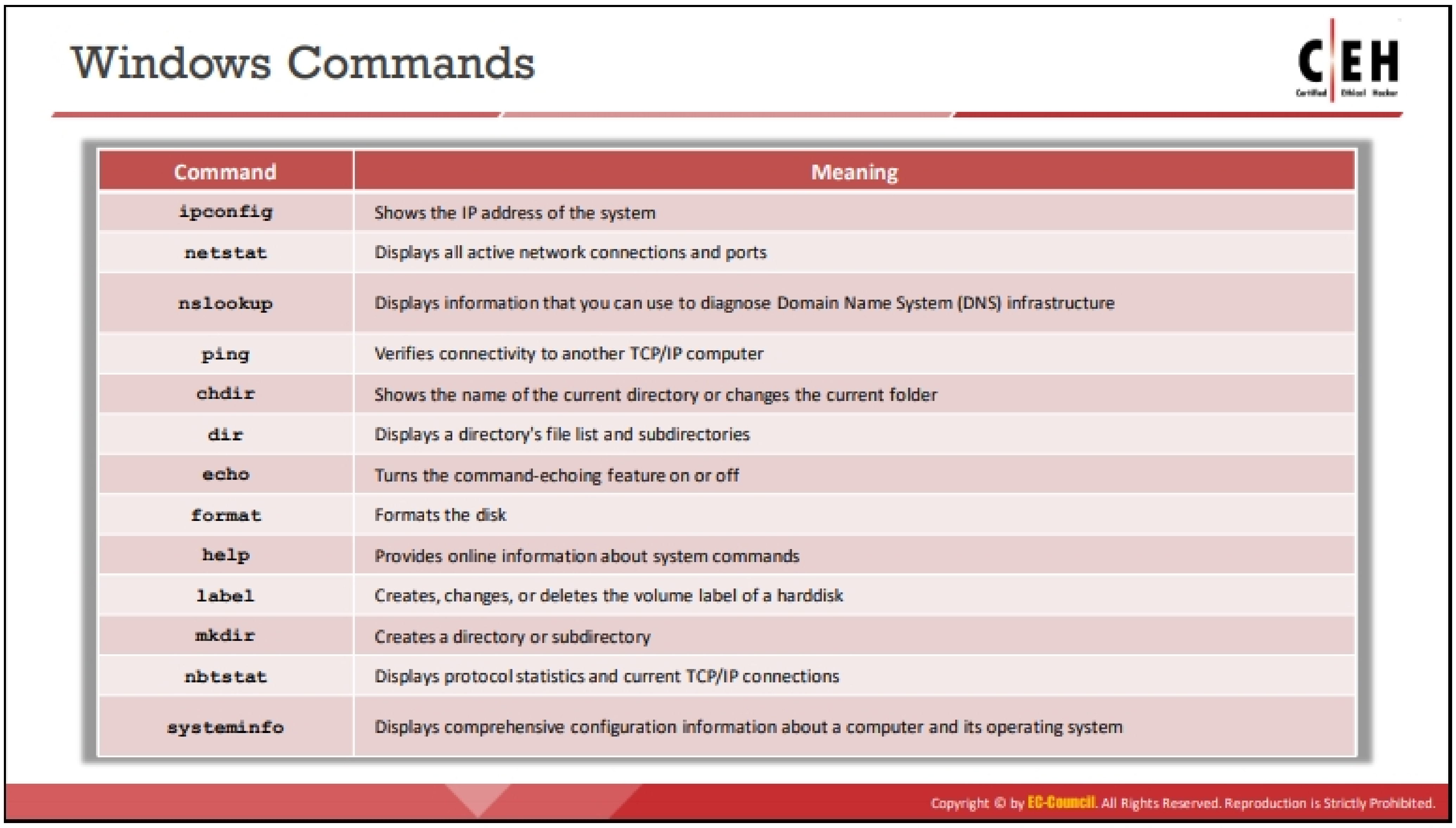
- A collection of Sub-Systems
- Has limited access to resources

Kernel Mode

- HAL, Kernel, executive
- Unrestricted access to system memory and external devices

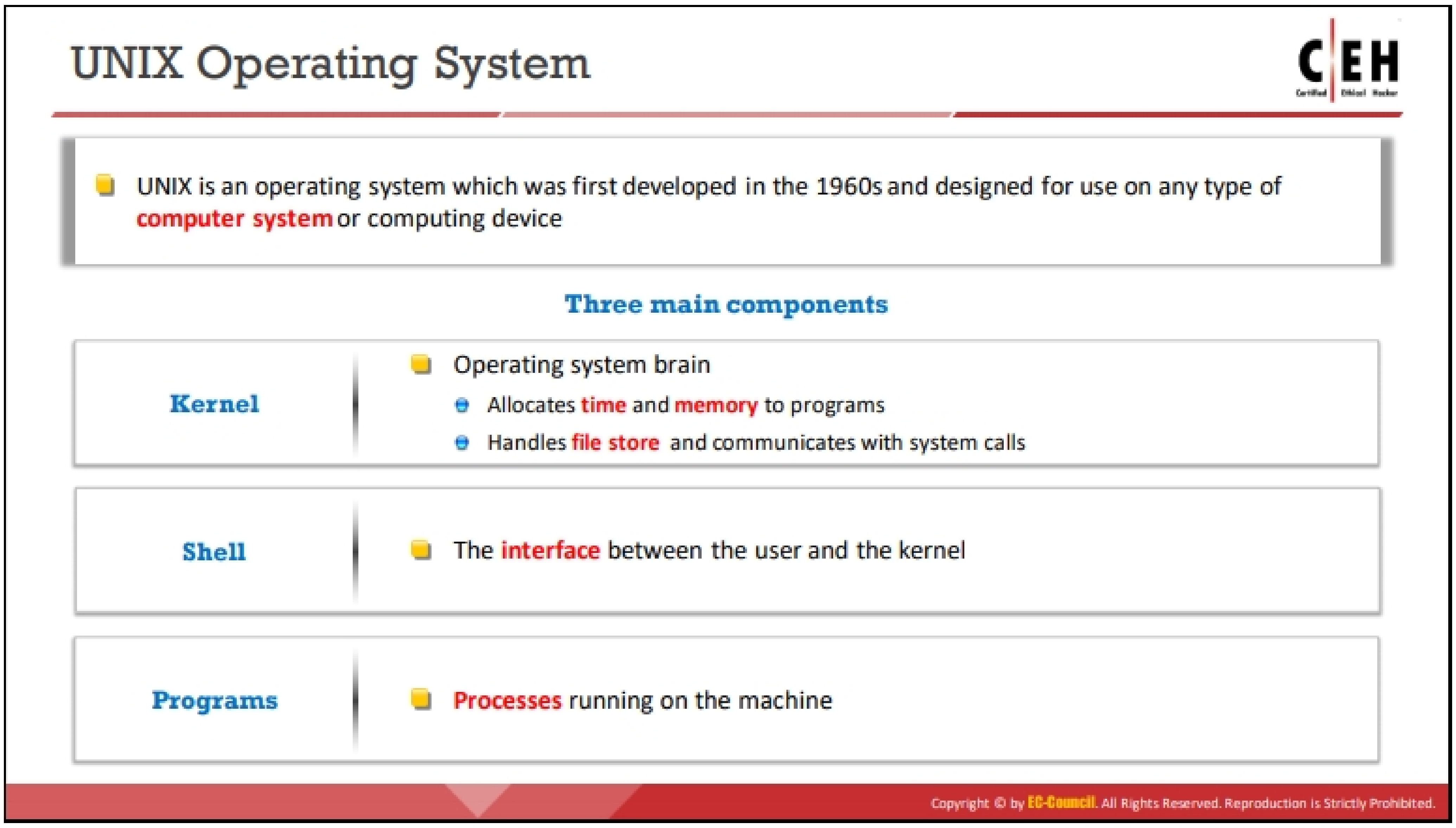
Windows Architecture
Win32 Application
POSIX Application
OS/2 Application
Work Station Service
Server Service
Security
Win32
POSIX
OS/2
Integral Subsystems
Environment Subsystems
User Mode
Executive Services
I/O Manager
Security Reference Monitor
IPC Manager
Virtual Memory Manager (VMM)
Process Manager
PnP Manager
Power Manager
Windows Manager
GDI
Object Manager
Executive
Kernel Mode Drivers
Microkernel
Hardware Abstraction Layer (HAL)
Kernel Mode
Hardware

Notes: ____



Windows Commands

Command	Meaning
`ipconfig`	Shows the IP address of the system
`netstat`	Displays all active network connections and ports
`nslookup`	Displays information that you can use to diagnose Domain Name System (DNS) infrastructure
`ping`	Verifies connectivity to another TCP/IP computer
`chdir`	Shows the name of the current directory or changes the current folder
`dir`	Displays a directory's file list and subdirectories
`echo`	Turns the command-echoing feature on or off
`format`	Formats the disk
`help`	Provides online information about system commands
`label`	Creates, changes, or deletes the volume label of a harddisk
`mkdir`	Creates a directory or subdirectory
`nbtstat`	Displays protocol statistics and current TCP/IP connections
`systeminfo`	Displays comprehensive configuration information about a computer and its operating system



UNIX Operating System

- UNIX is an operating system which was first developed in the 1960s and designed for use on any type of computer system or computing device

Three main components

Kernel

- Operating system brain
  - Allocates time and memory to programs
  - Handles file store and communicates with system calls

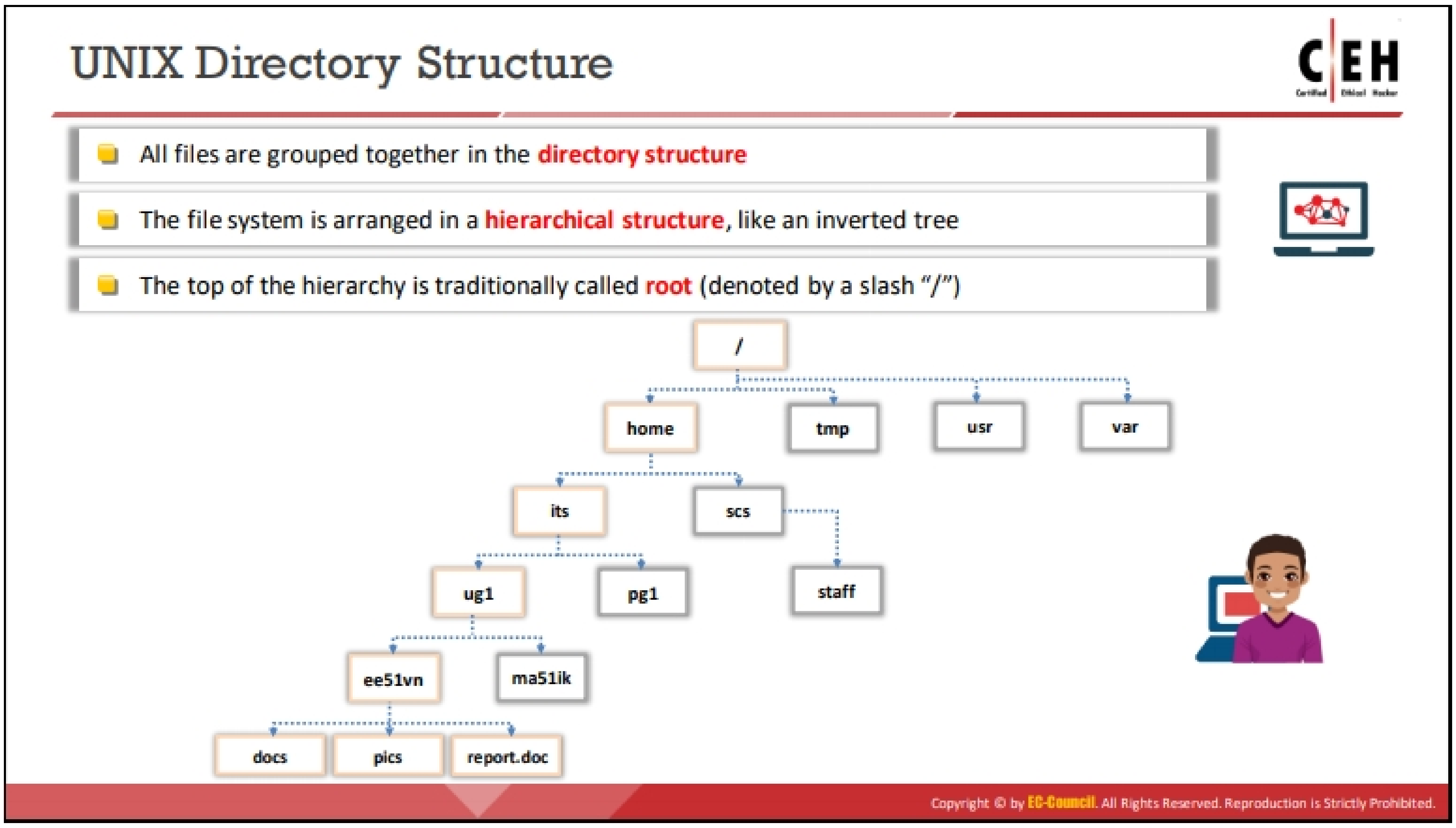
Shell

- The interface between the user and the kernel

Programs

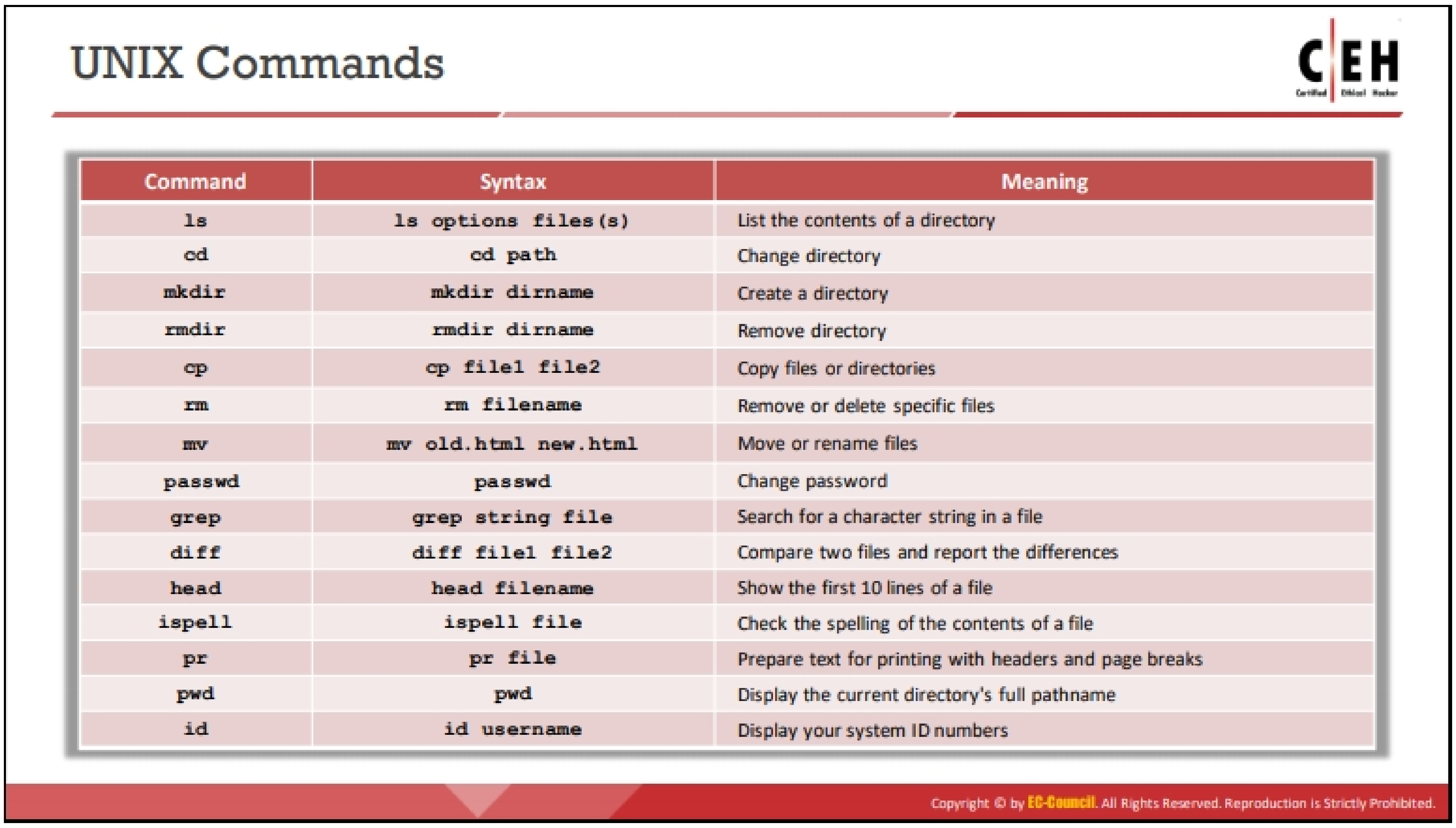
- Processes running on the machine

Notes:



UNIX Directory Structure

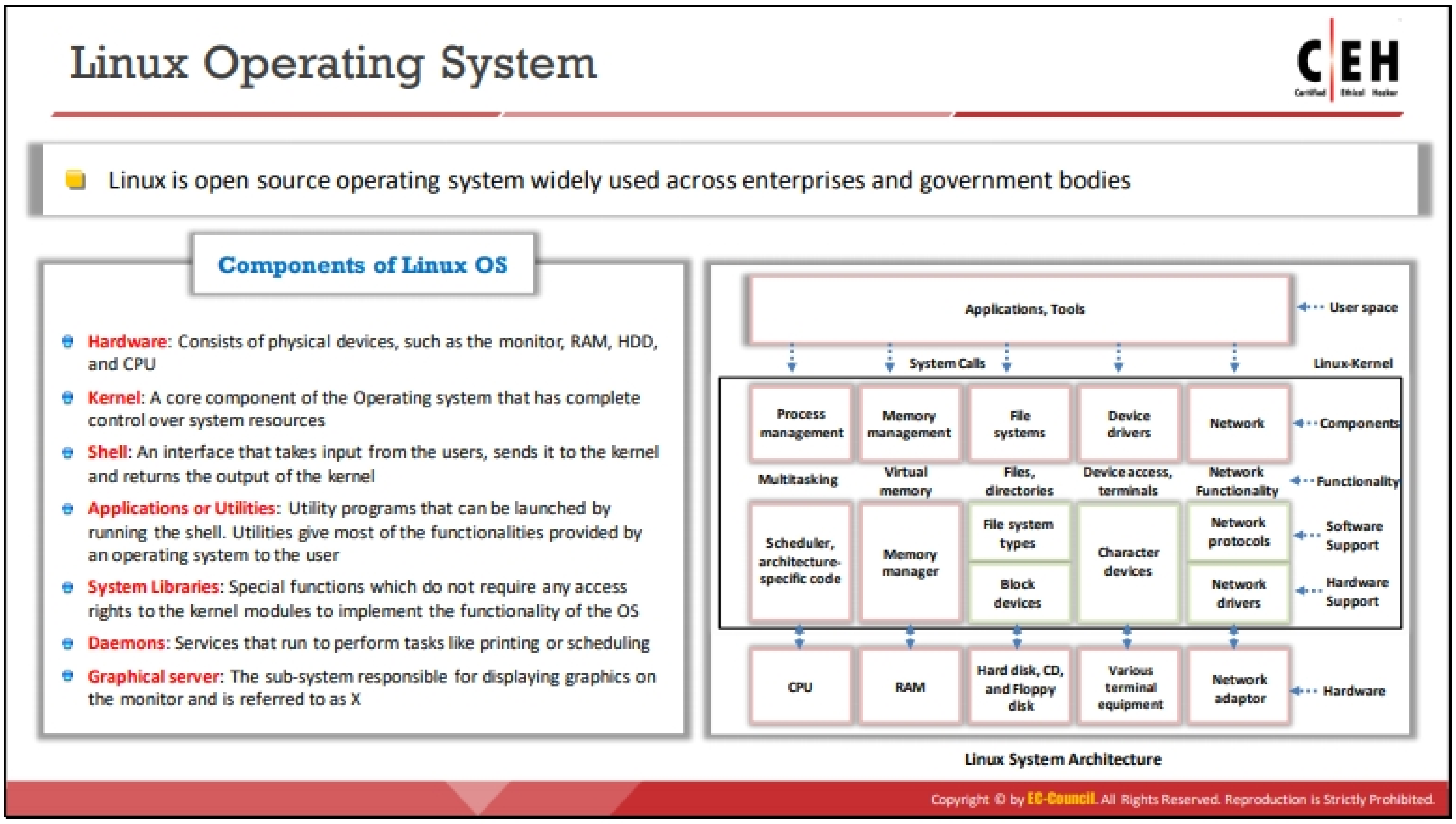
- All files are grouped together in the **directory structure**
- The file system is arranged in a **hierarchical structure**, like an inverted tree
- The top of the hierarchy is traditionally called **root** (denoted by a slash "/")



UNIX Commands

Command	Syntax	Meaning
`ls`	`ls options files(s)`	List the contents of a directory
`cd`	`cd path`	Change directory
`mkdir`	`mkdir dirname`	Create a directory
`rmdir`	`rmdir dirname`	Remove directory
`cp`	`cp file1 file2`	Copy files or directories
`rm`	`rm filename`	Remove or delete specific files
`mv`	`mv old.html new.html`	Move or rename files
`passwd`	`passwd`	Change password
`grep`	`grep string file`	Search for a character string in a file
`diff`	`diff file1 file2`	Compare two files and report the differences
`head`	`head filename`	Show the first 10 lines of a file
`ispell`	`ispell file`	Check the spelling of the contents of a file
`pr`	`pr file`	Prepare text for printing with headers and page breaks
`pwd`	`pwd`	Display the current directory's full pathname
`id`	`id username`	Display your system ID numbers

Notes: ____



Linux Operating System

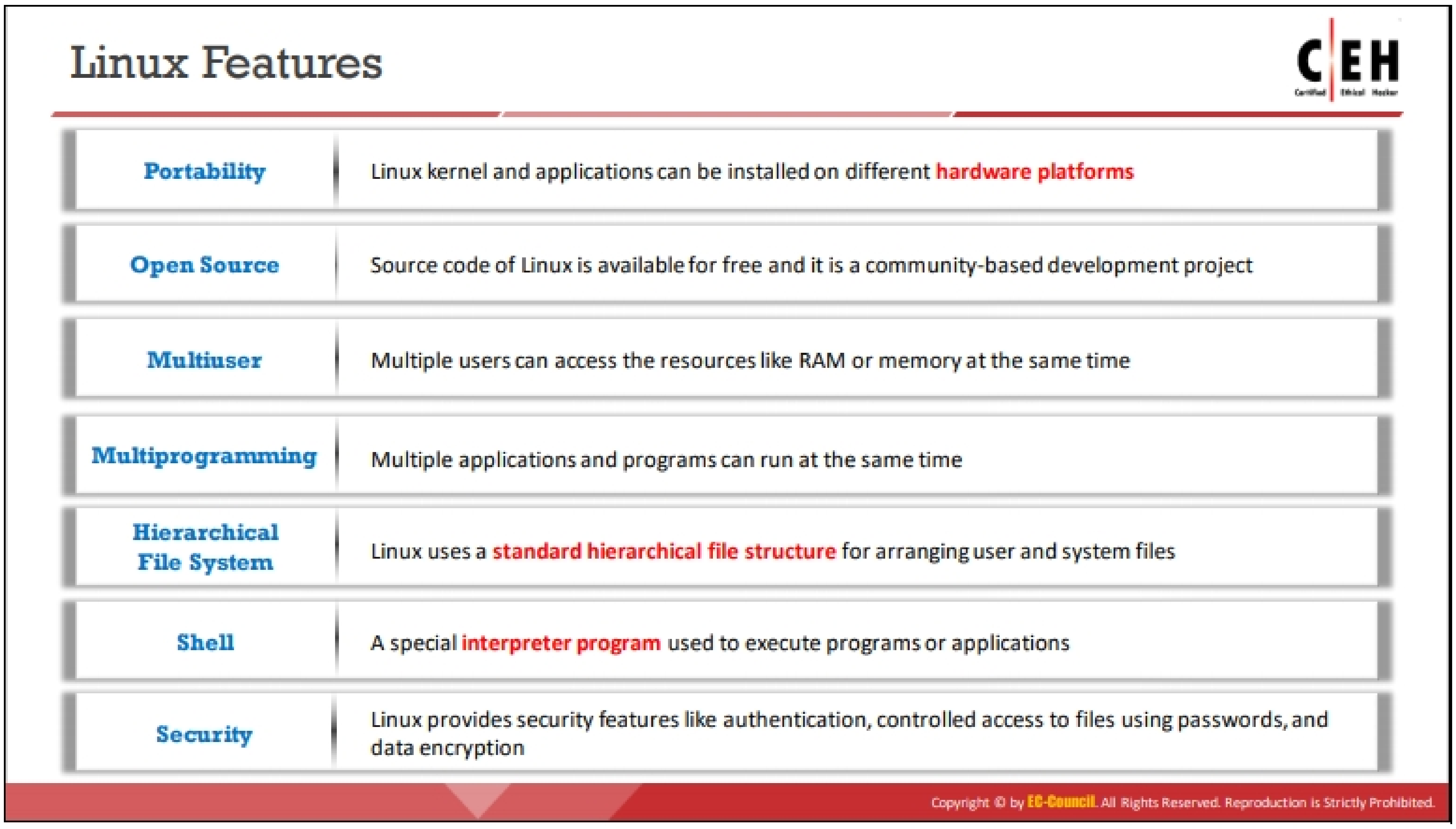
- Linux is open source operating system widely used across enterprises and government bodies

Components of Linux OS

- **Hardware**: Consists of physical devices, such as the monitor, RAM, HDD, and CPU
- **Kernel**: A core component of the Operating system that has complete control over system resources
- **Shell**: An interface that takes input from the users, sends it to the kernel and returns the output of the kernel
- **Applications or Utilities**: Utility programs that can be launched by running the shell. Utilities give most of the functionalities provided by an operating system to the user
- **System Libraries**: Special functions which do not require any access rights to the kernel modules to implement the functionality of the OS
- **Daemons**: Services that run to perform tasks like printing or scheduling
- **Graphical server**: The sub-system responsible for displaying graphics on the monitor and is referred to as X

Applications, Tools
User space
System Calls
Linux-Kernel
Process management
Memory management
File systems
Device drivers
Network
Components
Multitasking
Virtual memory
Files, directories
Device access, terminals
Network Functionality
Functionality
Scheduler, architecture-specific code
Memory manager
File system types
Block devices
Character devices
Network protocols
Network drivers
Software Support
Hardware Support
CPU
RAM
Hard disk, CD, and Floppy disk
Various terminal equipment
Network adaptor
Hardware

Linux System Architecture



Linux Features

Portability	Linux kernel and applications can be installed on different **hardware platforms**
Open Source	Source code of Linux is available for free and it is a community-based development project
Multiuser	Multiple users can access the resources like RAM or memory at the same time
Multiprogramming	Multiple applications and programs can run at the same time
Hierarchical File System	Linux uses a **standard hierarchical file structure** for arranging user and system files
Shell	A special **interpreter program** used to execute programs or applications
Security	Linux provides security features like authentication, controlled access to files using passwords, and data encryption

Notes: ____

____

____

____

____

____

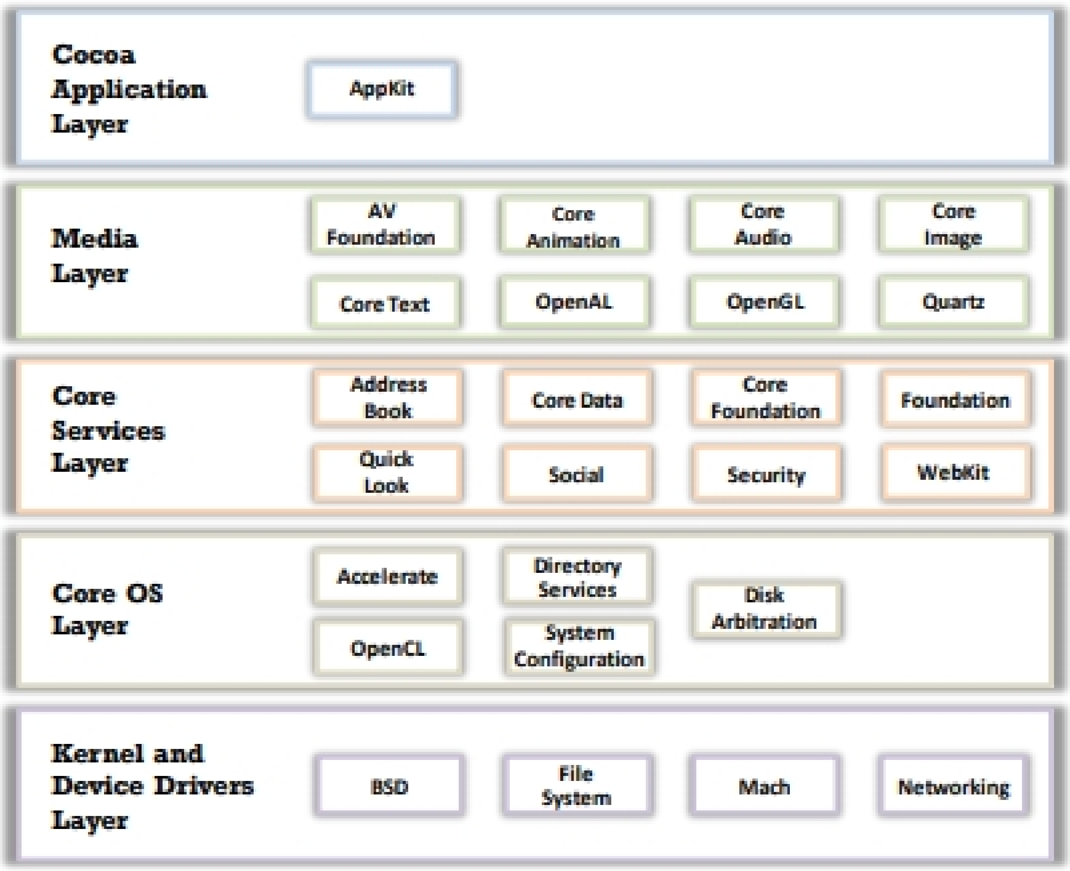
MAC OS X Operating System

- MAC OS X is a series of closed-source graphical operating systems developed by Apple Inc.
- It is the primary operating system for Apple's Mac computers
- It can offer a more stable and reliable platform and supports pre-emptive multitasking and memory protection

Layers of MAC OS X

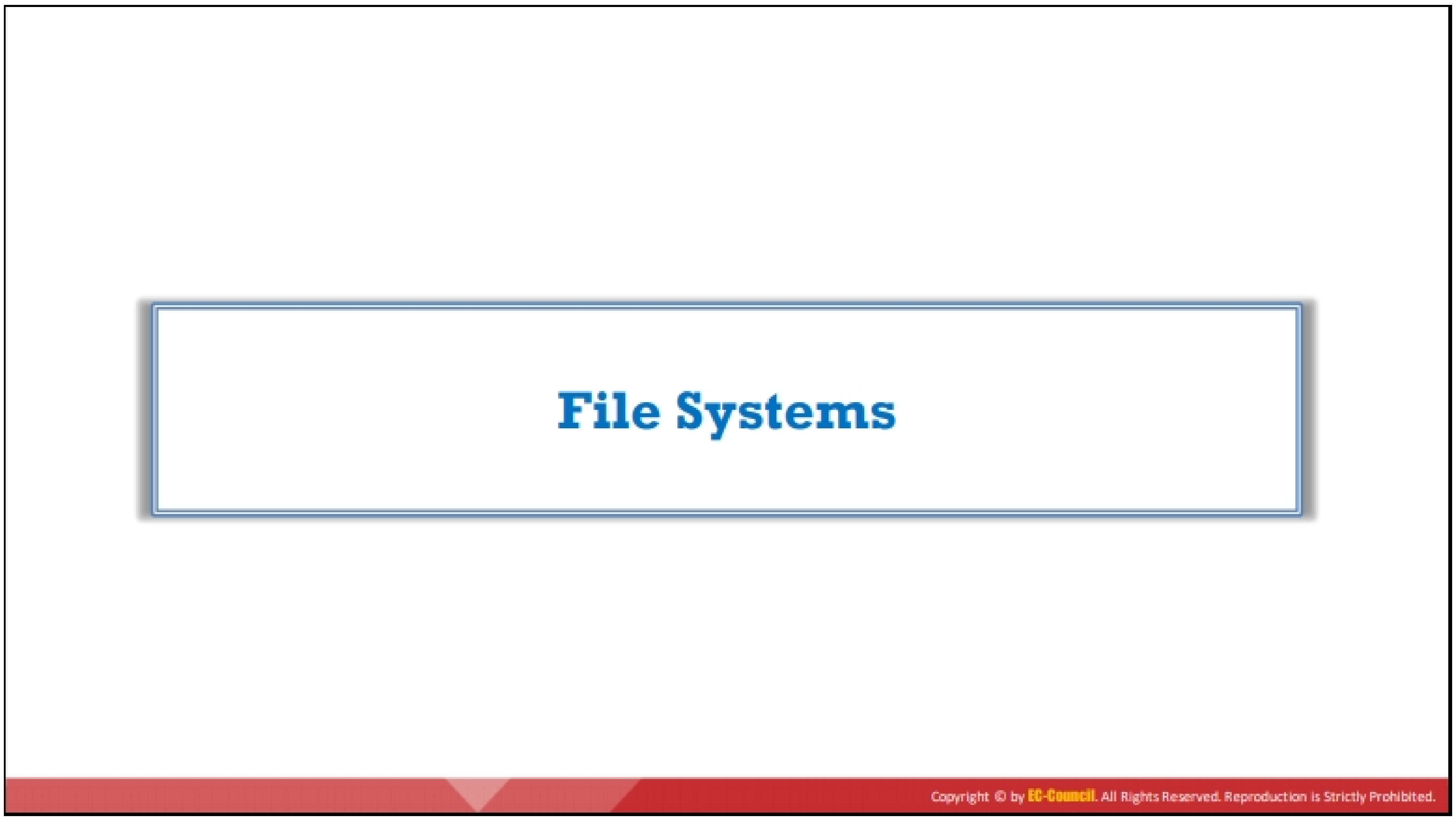
- **Cocoa Application layer**: Encompasses technologies for building an app's user interface
- **Media layer**: Incorporates specialized technologies for playing, recording, and editing audio and visual media
- **Core Services layer**: Comprises fundamental services and technologies ranging from Automatic Reference Counting to string manipulation and data formatting
- **Core OS layer**: Outlines programming interfaces related to hardware and networking
- **Kernel and Device Drivers layer**: Contains support for file systems, networking, security, IPC, programming languages, device drivers, and other tools

MAC OS X Layered Architecture

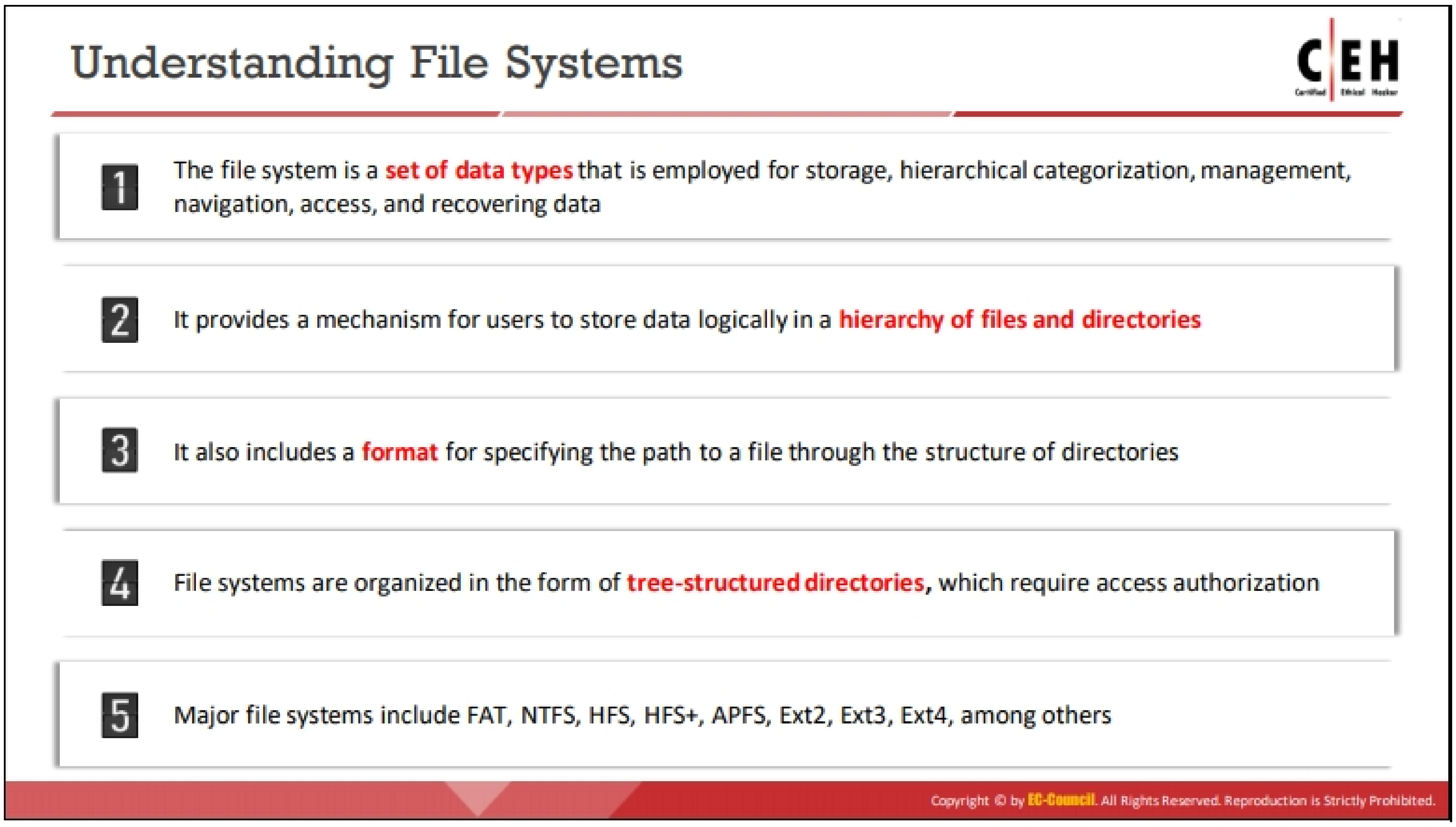


Cocoa Application Layer	AppKit			
Media Layer	AV Foundation	Core Animation	Core Audio	Core Image
	Core Text	OpenAL	OpenGL	Quartz
Core Services Layer	Address Book	Core Data	Core Foundation	Foundation
	Quick Look	Social	Security	WebKit
Core OS Layer	Accelerate	Directory Services	Disk Arbitration	
	OpenCL	System Configuration		
Kernel and Device Drivers Layer	BSD	File System	Mach	Networking

Notes:



File Systems



Understanding File Systems

1. The file system is a **set of data types** that is employed for storage, hierarchical categorization, management, navigation, access, and recovering data
2. It provides a mechanism for users to store data logically in a **hierarchy of files and directories**
3. It also includes a **format** for specifying the path to a file through the structure of directories
4. File systems are organized in the form of **tree-structured directories**, which require access authorization
5. Major file systems include FAT, NTFS, HFS, HFS+, APFS, Ext2, Ext3, Ext4, among others

Notes: ____

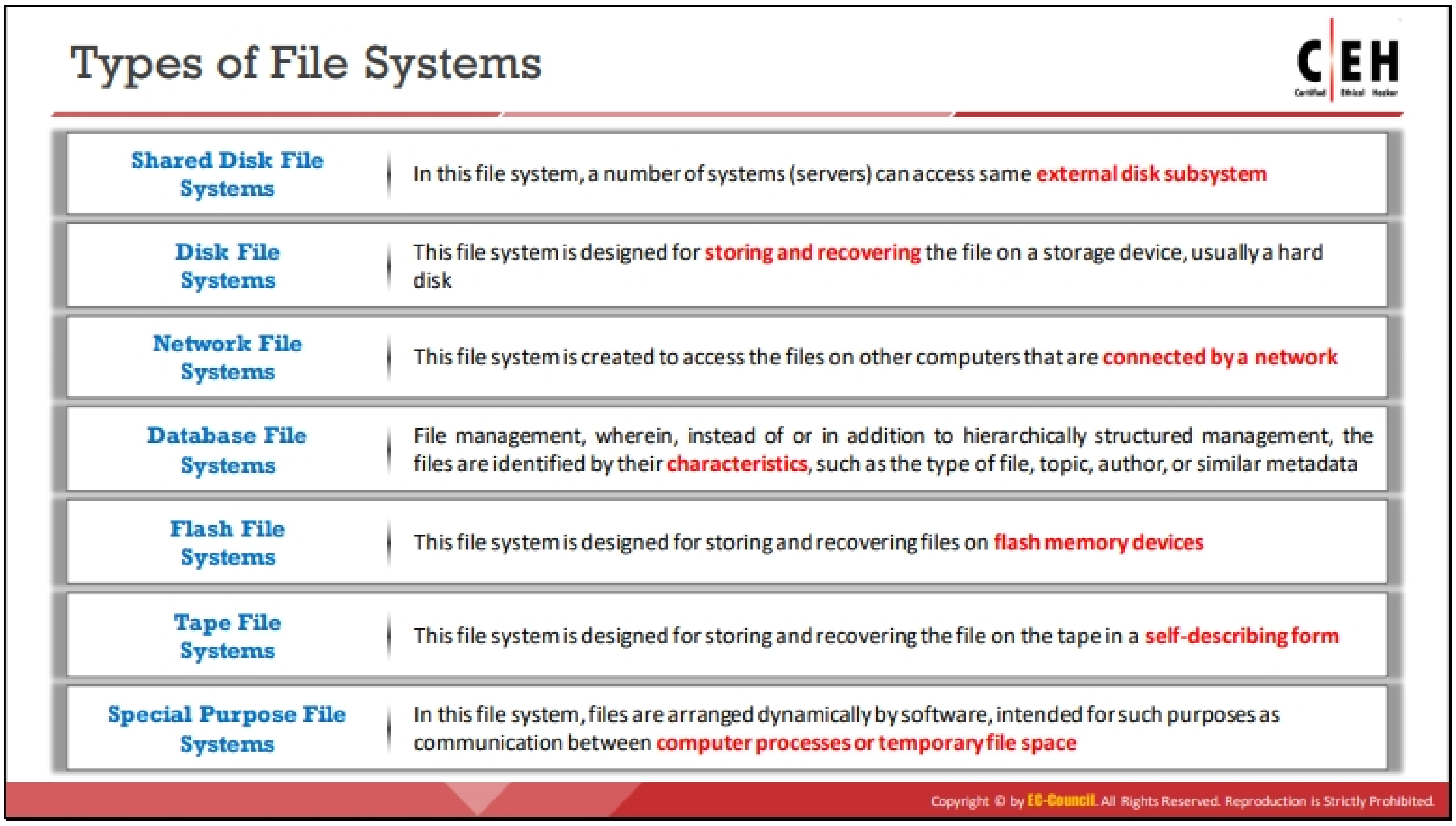
____

____

____

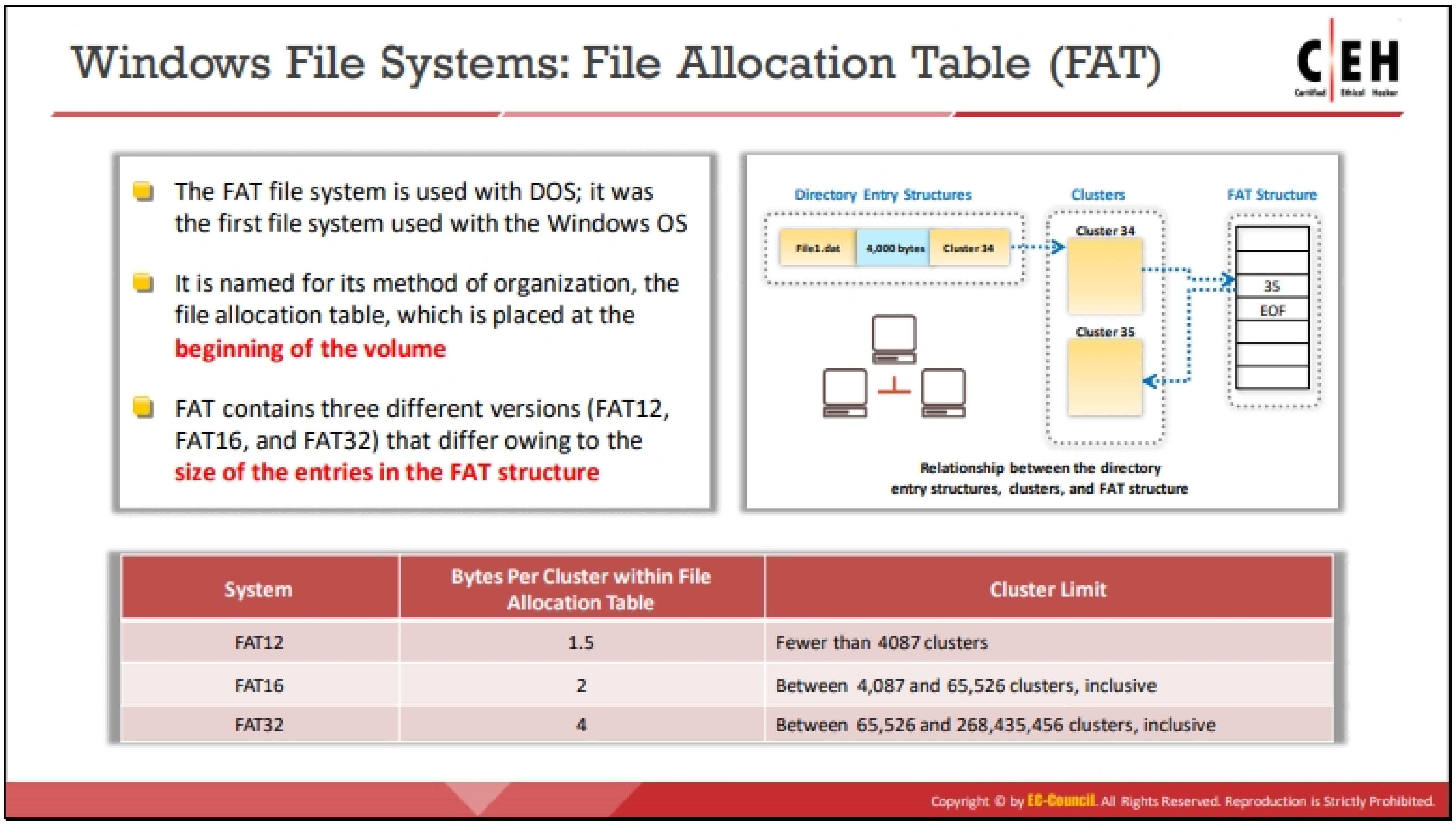
____

____



Types of File Systems

Shared Disk File Systems	In this file system, a number of systems (servers) can access same **external disk subsystem**
Disk File Systems	This file system is designed for **storing and recovering** the file on a storage device, usually a hard disk
Network File Systems	This file system is created to access the files on other computers that are **connected by a network**
Database File Systems	File management, wherein, instead of or in addition to hierarchically structured management, the files are identified by their **characteristics**, such as the type of file, topic, author, or similar metadata
Flash File Systems	This file system is designed for storing and recovering files on **flash memory devices**
Tape File Systems	This file system is designed for storing and recovering the file on the tape in a **self-describing form**
Special Purpose File Systems	In this file system, files are arranged dynamically by software, intended for such purposes as communication between **computer processes or temporary file space**



Windows File Systems: File Allocation Table (FAT)

- The FAT file system is used with DOS; it was the first file system used with the Windows OS
- It is named for its method of organization, the file allocation table, which is placed at the **beginning of the volume**
- FAT contains three different versions (FAT12, FAT16, and FAT32) that differ owing to the **size of the entries in the FAT structure**

Relationship between the directory entry structures, clusters, and FAT structure

System	Bytes Per Cluster within File Allocation Table	Cluster Limit
FAT12	1.5	Fewer than 4087 clusters
FAT16	2	Between 4,087 and 65,526 clusters, inclusive
FAT32	4	Between 65,526 and 268,435,456 clusters, inclusive

Notes: ____

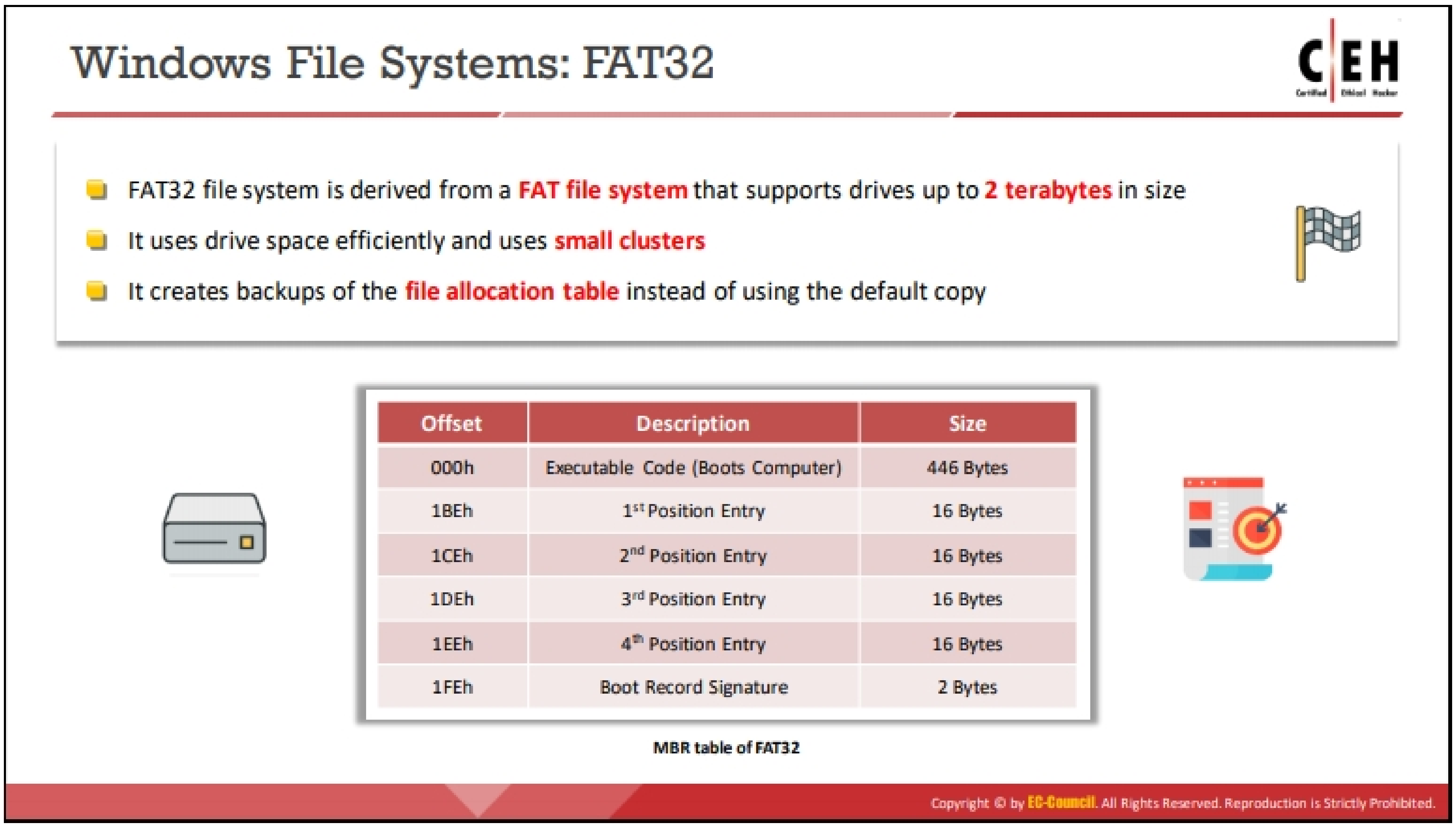
____

____

____

____

____

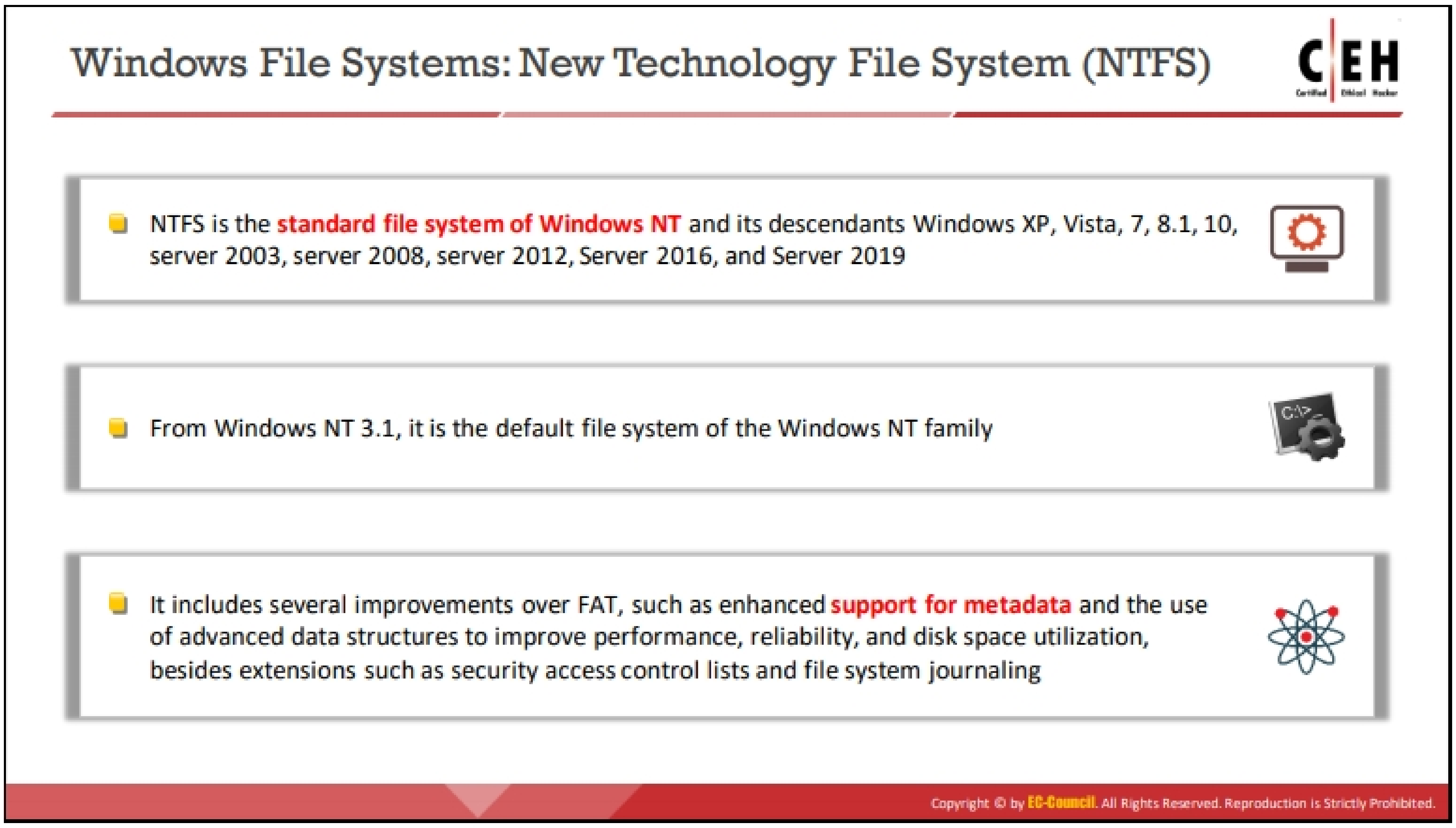


Windows File Systems: FAT32

- FAT32 file system is derived from a **FAT file system** that supports drives up to **2 terabytes** in size
- It uses drive space efficiently and uses **small clusters**
- It creates backups of the **file allocation table** instead of using the default copy

Offset	Description	Size
000h	Executable Code (Boots Computer)	446 Bytes
1BEh	1st Position Entry	16 Bytes
1CEh	2nd Position Entry	16 Bytes
1DEh	3rd Position Entry	16 Bytes
1EEh	4th Position Entry	16 Bytes
1FEh	Boot Record Signature	2 Bytes

MBR table of FAT32



Windows File Systems: New Technology File System (NTFS)

- NTFS is the **standard file system of Windows NT** and its descendants Windows XP, Vista, 7, 8.1, 10, server 2003, server 2008, server 2012, Server 2016, and Server 2019

- From Windows NT 3.1, it is the default file system of the Windows NT family

- It includes several improvements over FAT, such as enhanced **support for metadata** and the use of advanced data structures to improve performance, reliability, and disk space utilization, besides extensions such as security access control lists and file system journaling

Notes: ____

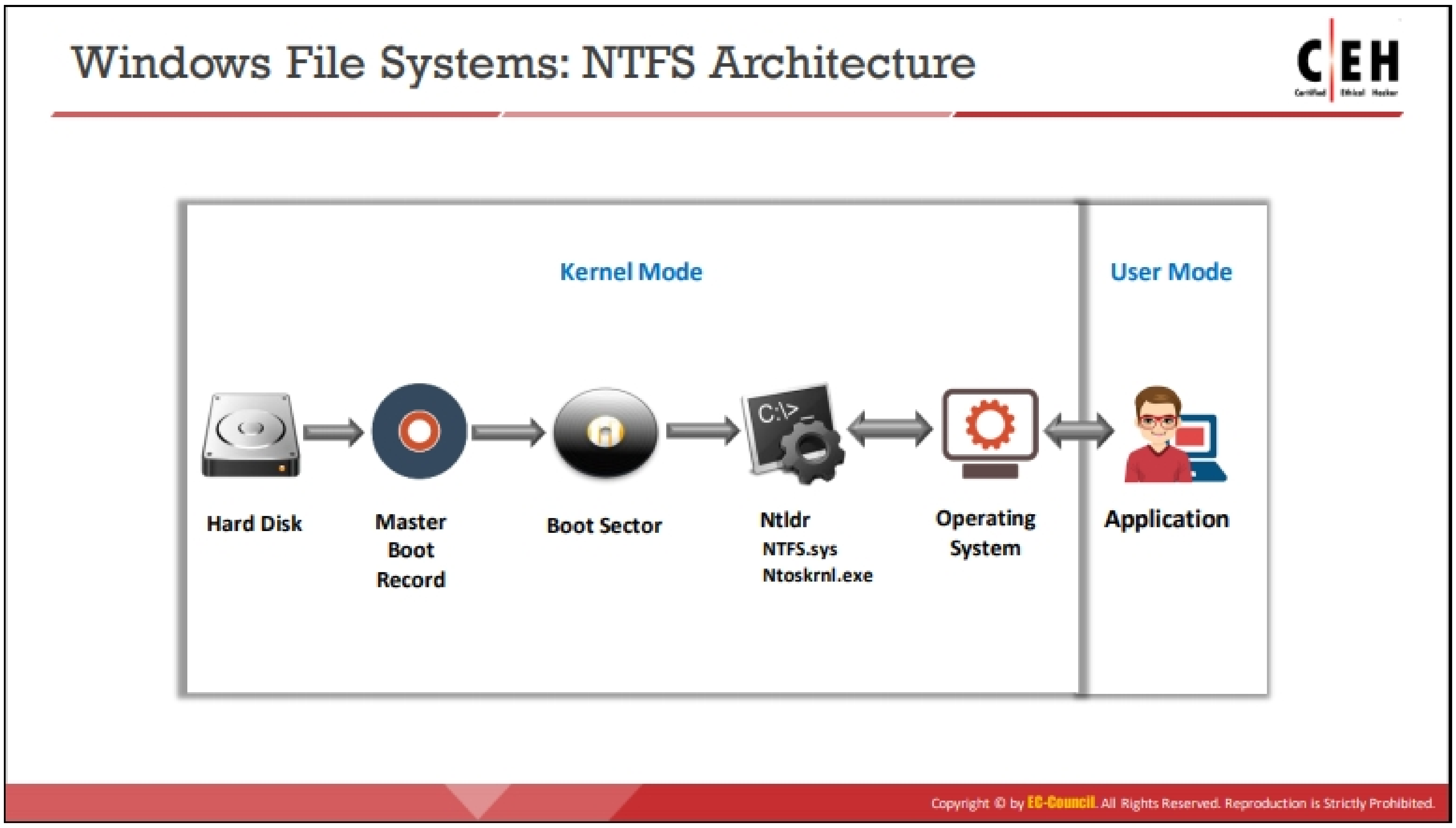
____

____

____

____

____

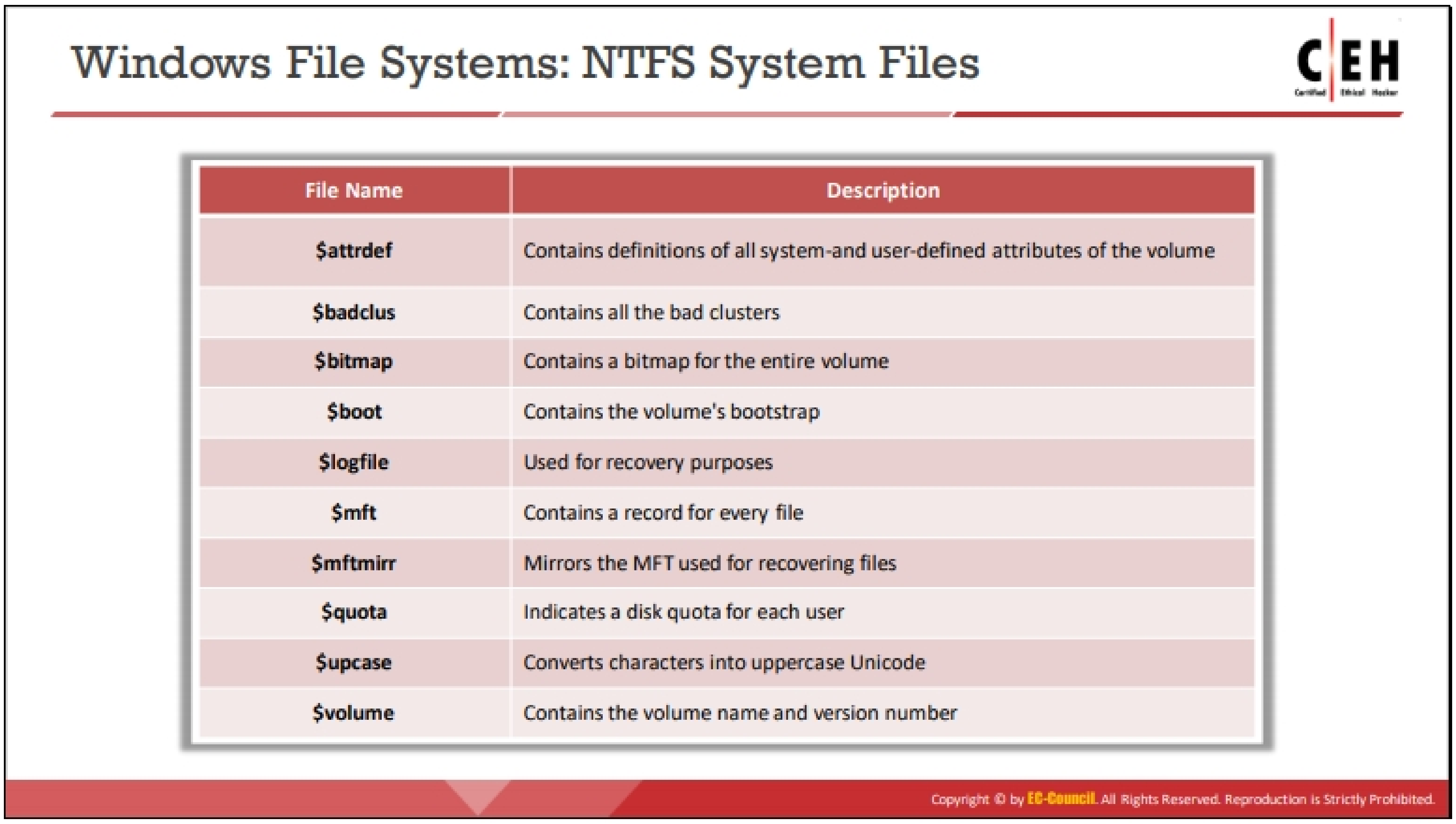


Windows File Systems: NTFS Architecture

Kernel Mode

User Mode

Hard Disk → **Master Boot Record** → **Boot Sector** → **Ntldr** NTFS.sys Ntoskrnl.exe ↔ **Operating System** ↔ **Application**



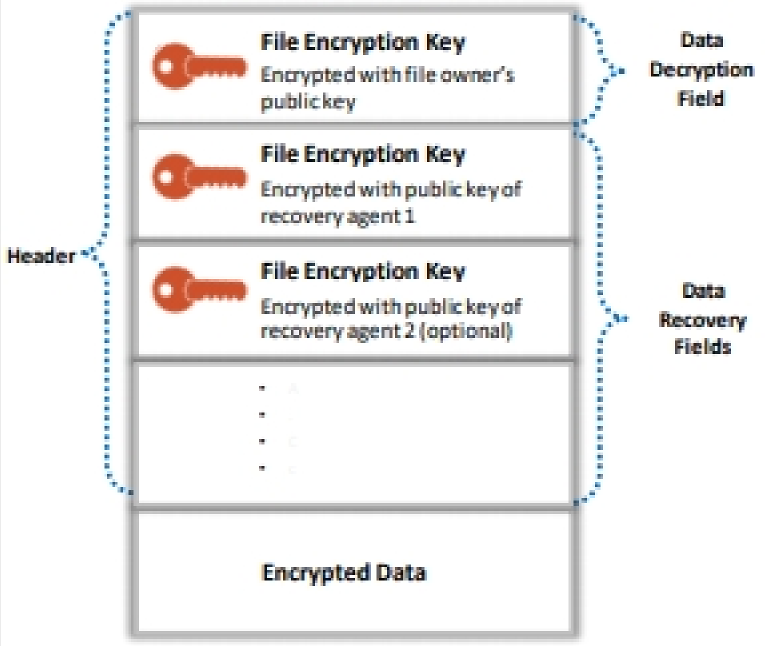
Windows File Systems: NTFS System Files

File Name	Description
$attrdef	Contains definitions of all system-and user-defined attributes of the volume
$badclus	Contains all the bad clusters
$bitmap	Contains a bitmap for the entire volume
$boot	Contains the volume's bootstrap
$logfile	Used for recovery purposes
$mft	Contains a record for every file
$mftmirr	Mirrors the MFT used for recovering files
$quota	Indicates a disk quota for each user
$upcase	Converts characters into uppercase Unicode
$volume	Contains the volume name and version number

Notes: ____

Windows File Systems: Encrypting File Systems (EFS)

- The Encrypting File System (EFS) was first introduced in version 3.0 of NTFS, which offers filesystem-level encryption
- This encryption technology maintains a **level of transparency** to the user who encrypted the file, which implies that there is no need for users to decrypt the file and access it for making changes
- After a user is done with the file, the **encryption policy** is automatically restored
- When any unauthorized user tries to access an **encrypted file**, they are **denied access**
- To enable the encryption and decryption facilities, a user has to set the **encryption attributes** of the files and folders that the user wants to encrypt or decrypt



Header

File Encryption Key
Encrypted with file owner's public key

File Encryption Key
Encrypted with public key of recovery agent 1

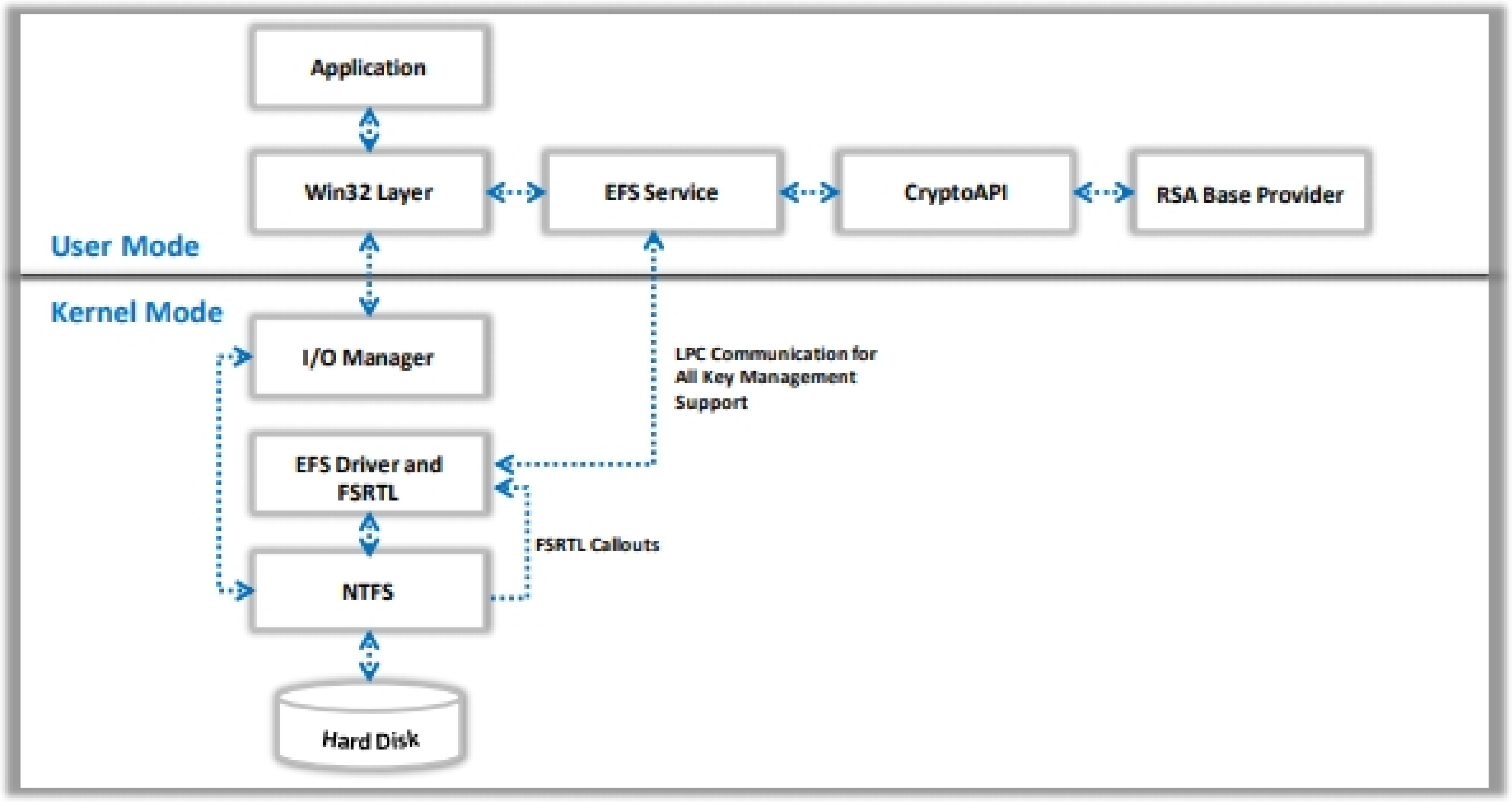
File Encryption Key
Encrypted with public key of recovery agent 2 (optional)

Encrypted Data

Data Decryption Field

Data Recovery Fields

Windows File Systems: Components of EFS



Application
Win32 Layer
EFS Service
CryptoAPI
RSA Base Provider
User Mode
Kernel Mode
I/O Manager
LPC Communication for All Key Management Support
EFS Driver and FSRTL
FSRTL Callouts
NTFS
Hard Disk

Notes: ____

____

____

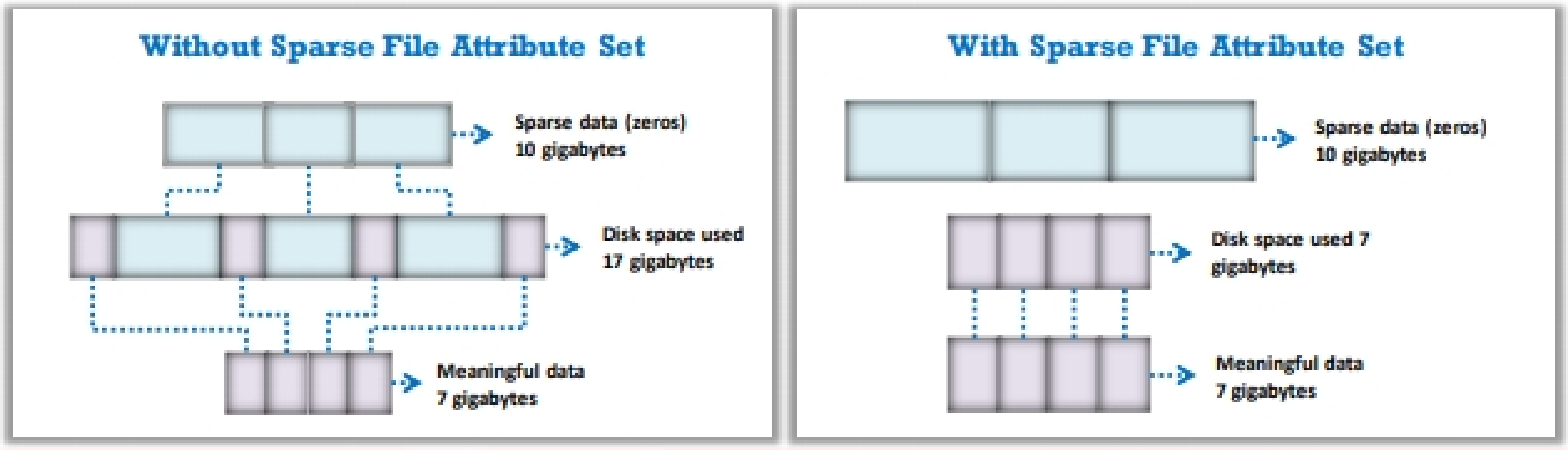
____

____

____

Windows File Systems: Sparse Files

- Sparse files provide a method of **saving disk space** for files by allowing the I/O subsystem to allocate only meaningful (nonzero) data
- If an NTFS file is marked as sparse, it assigns a **hard disk cluster** only for the data defined by the application
- The non-defined data of the file are represented by **non-allocated space** on the disk



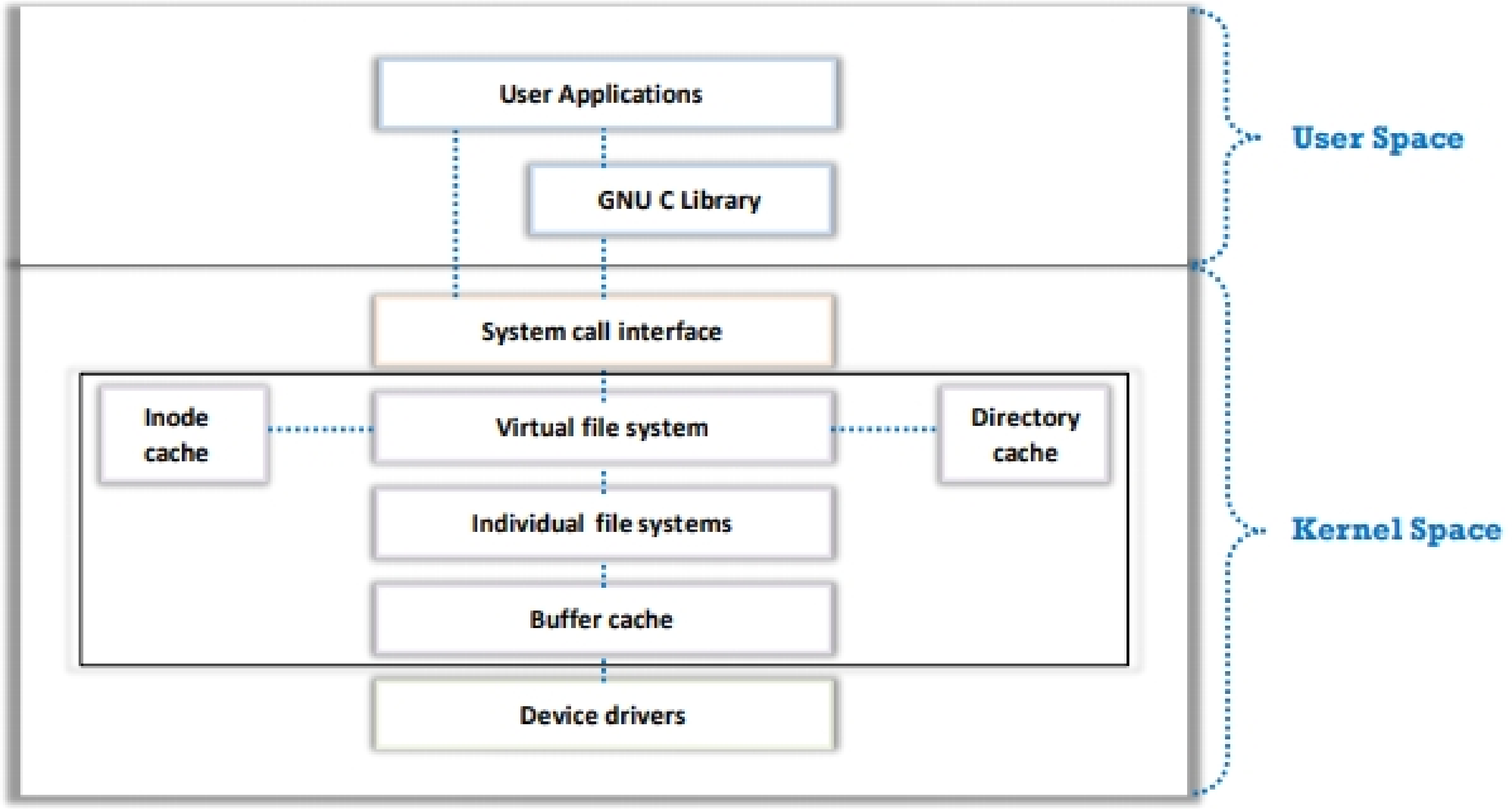
Without Sparse File Attribute Set

Sparse data (zeros) 10 gigabytes
Disk space used 17 gigabytes
Meaningful data 7 gigabytes

With Sparse File Attribute Set

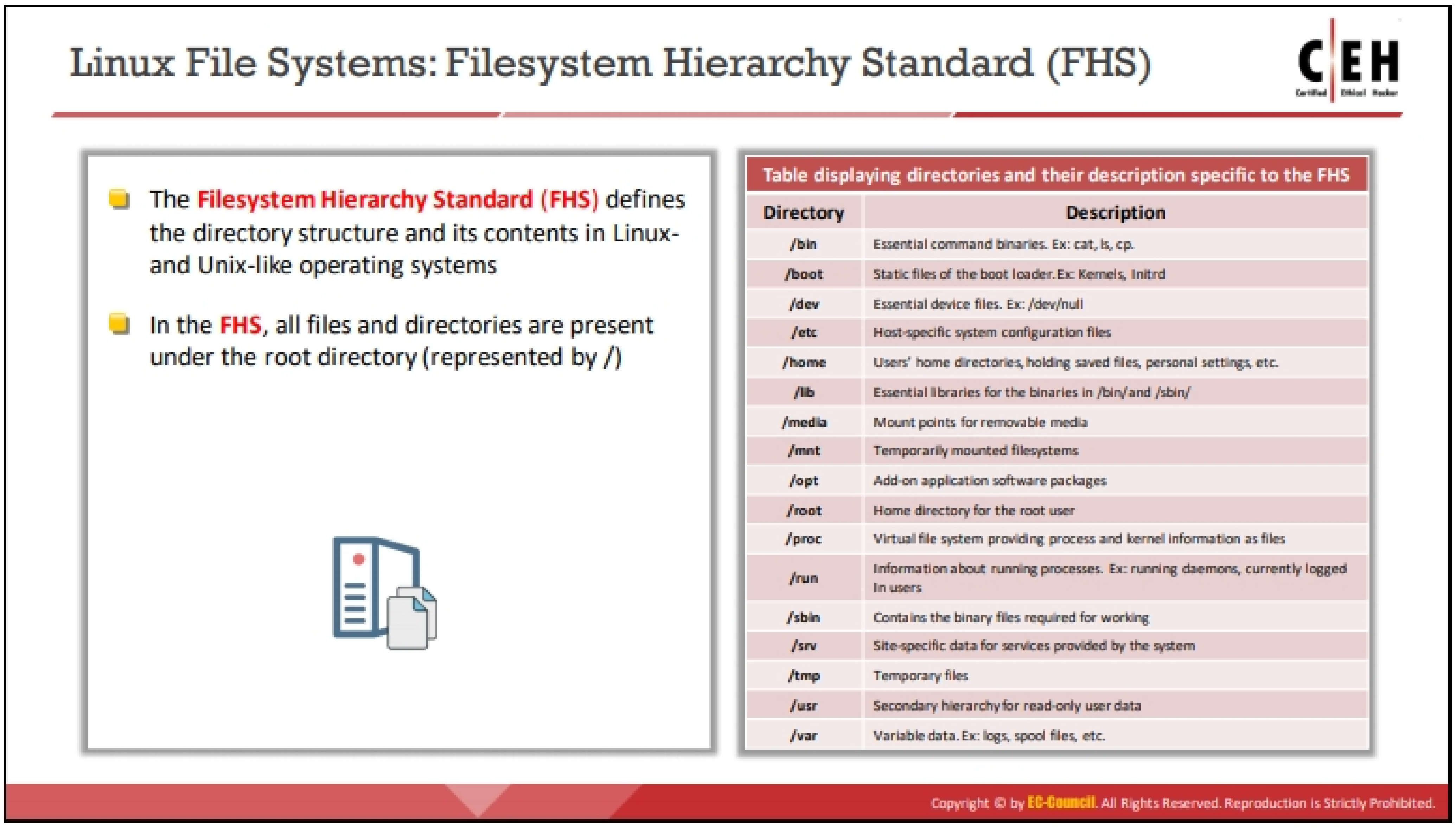
Sparse data (zeros) 10 gigabytes
Disk space used 7 gigabytes
Meaningful data 7 gigabytes

Linux File Systems: Linux File System Architecture



User Applications
GNU C Library
User Space
System call interface
Inode cache
Virtual file system
Directory cache
Individual file systems
Buffer cache
Device drivers
Kernel Space

Notes:

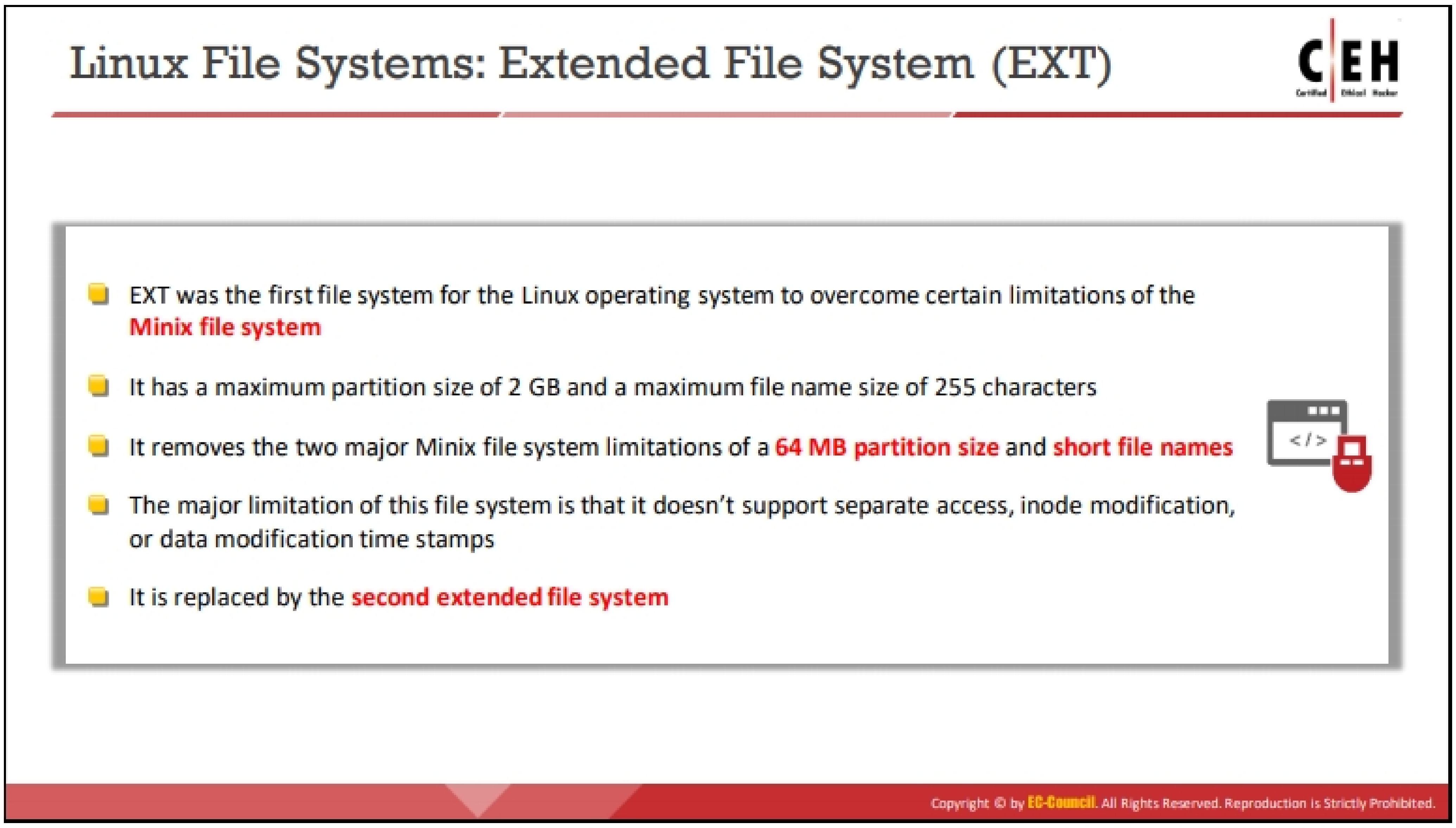


Linux File Systems: Filesystem Hierarchy Standard (FHS)

- The **Filesystem Hierarchy Standard (FHS)** defines the directory structure and its contents in Linux- and Unix-like operating systems
- In the **FHS**, all files and directories are present under the root directory (represented by /)

Table displaying directories and their description specific to the FHS

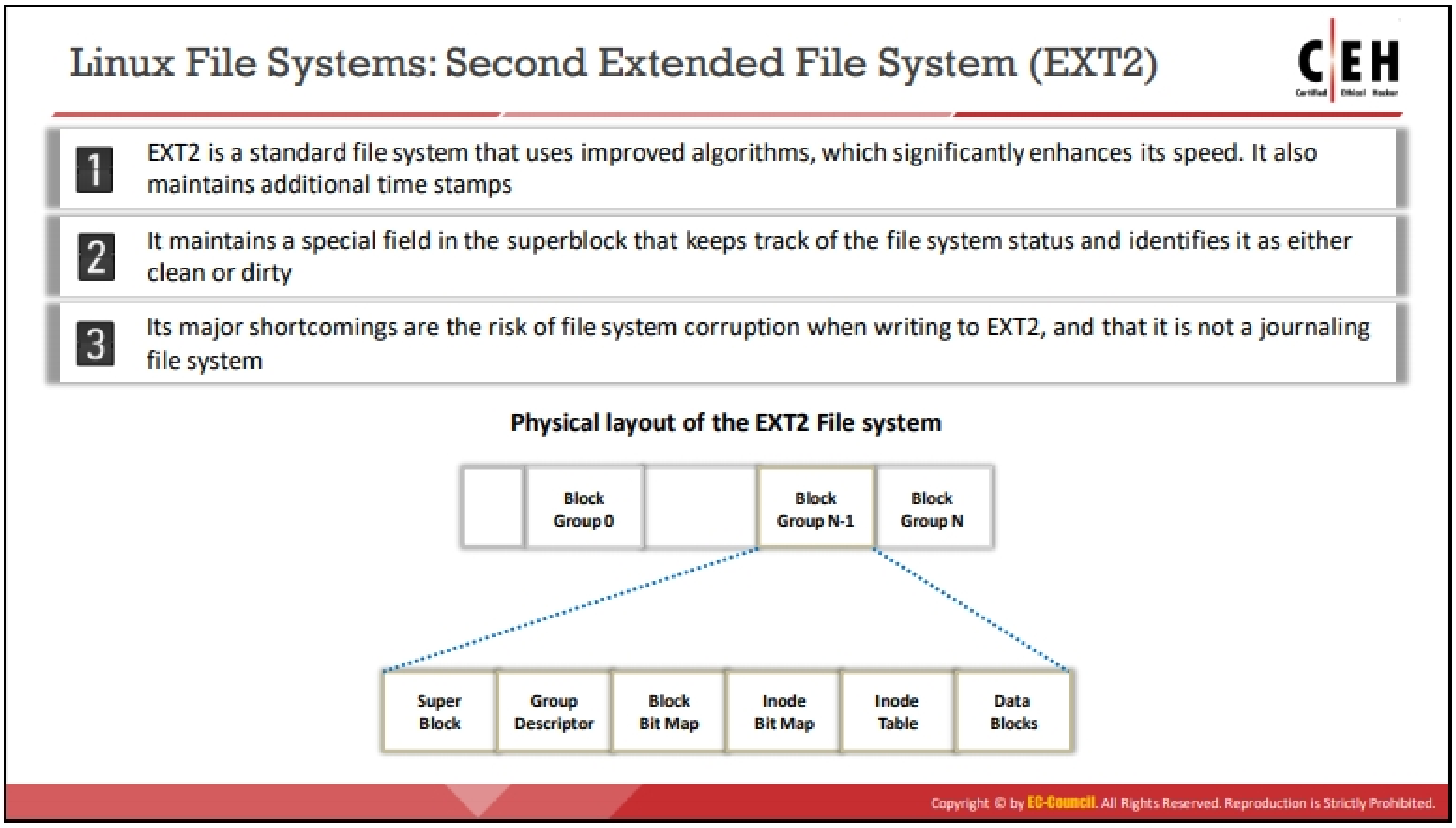
Directory	Description
/bin	Essential command binaries. Ex: cat, ls, cp.
/boot	Static files of the boot loader. Ex: Kernels, Initrd
/dev	Essential device files. Ex: /dev/null
/etc	Host-specific system configuration files
/home	Users' home directories, holding saved files, personal settings, etc.
/lib	Essential libraries for the binaries in /bin/ and /sbin/
/media	Mount points for removable media
/mnt	Temporarily mounted filesystems
/opt	Add-on application software packages
/root	Home directory for the root user
/proc	Virtual file system providing process and kernel information as files
/run	Information about running processes. Ex: running daemons, currently logged in users
/sbin	Contains the binary files required for working
/srv	Site-specific data for services provided by the system
/tmp	Temporary files
/usr	Secondary hierarchy for read-only user data
/var	Variable data. Ex: logs, spool files, etc.



Linux File Systems: Extended File System (EXT)

- EXT was the first file system for the Linux operating system to overcome certain limitations of the **Minix file system**
- It has a maximum partition size of 2 GB and a maximum file name size of 255 characters
- It removes the two major Minix file system limitations of a **64 MB partition size** and **short file names**
- The major limitation of this file system is that it doesn't support separate access, inode modification, or data modification time stamps
- It is replaced by the **second extended file system**

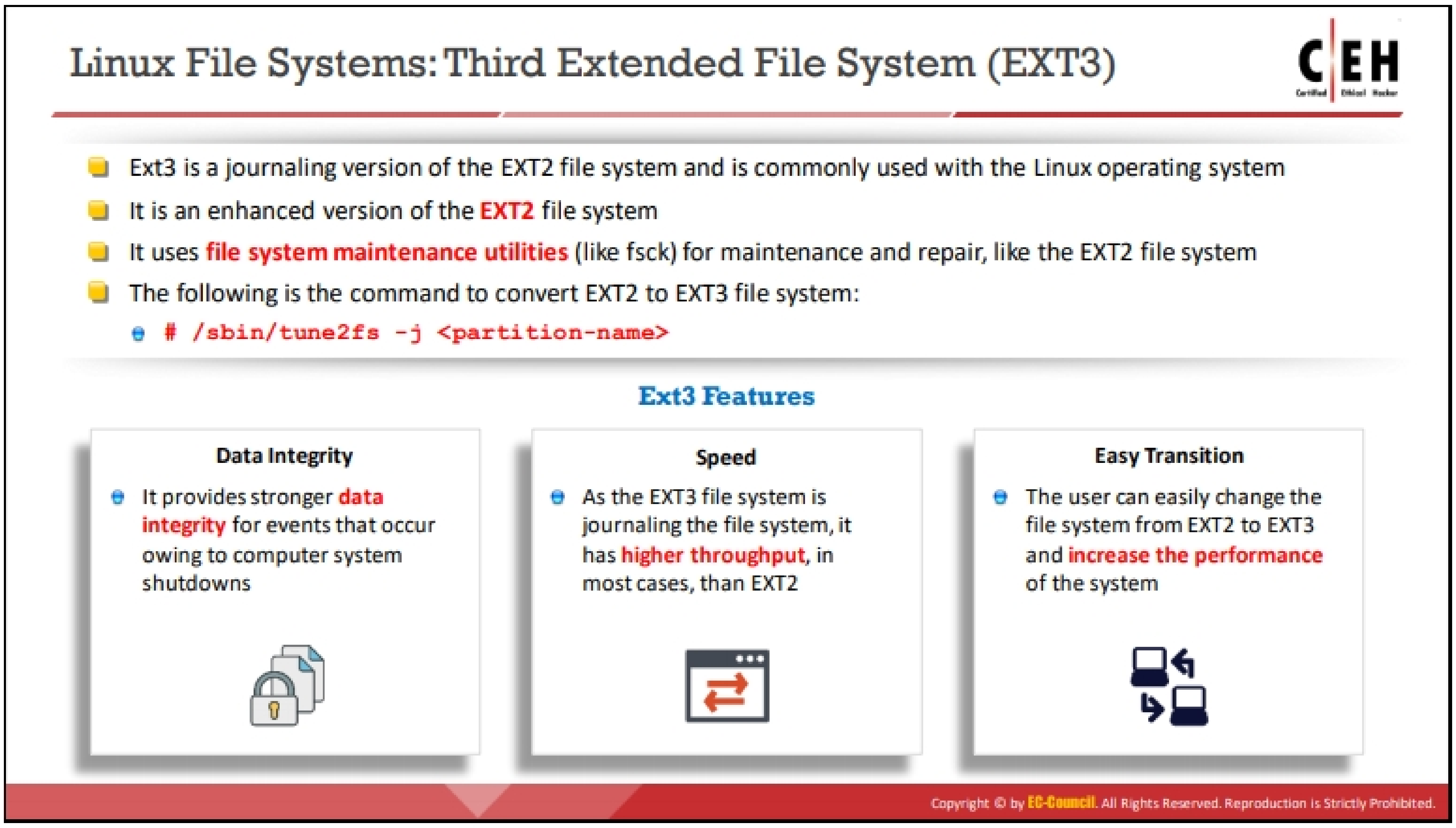
Notes: ____________________



Linux File Systems: Second Extended File System (EXT2)

1. EXT2 is a standard file system that uses improved algorithms, which significantly enhances its speed. It also maintains additional time stamps
2. It maintains a special field in the superblock that keeps track of the file system status and identifies it as either clean or dirty
3. Its major shortcomings are the risk of file system corruption when writing to EXT2, and that it is not a journaling file system

Physical layout of the EXT2 File system



Linux File Systems: Third Extended File System (EXT3)

- Ext3 is a journaling version of the EXT2 file system and is commonly used with the Linux operating system
- It is an enhanced version of the **EXT2** file system
- It uses **file system maintenance utilities** (like fsck) for maintenance and repair, like the EXT2 file system
- The following is the command to convert EXT2 to EXT3 file system:
  - `# /sbin/tune2fs -j <partition-name>`

Ext3 Features

Data Integrity

- It provides stronger **data integrity** for events that occur owing to computer system shutdowns

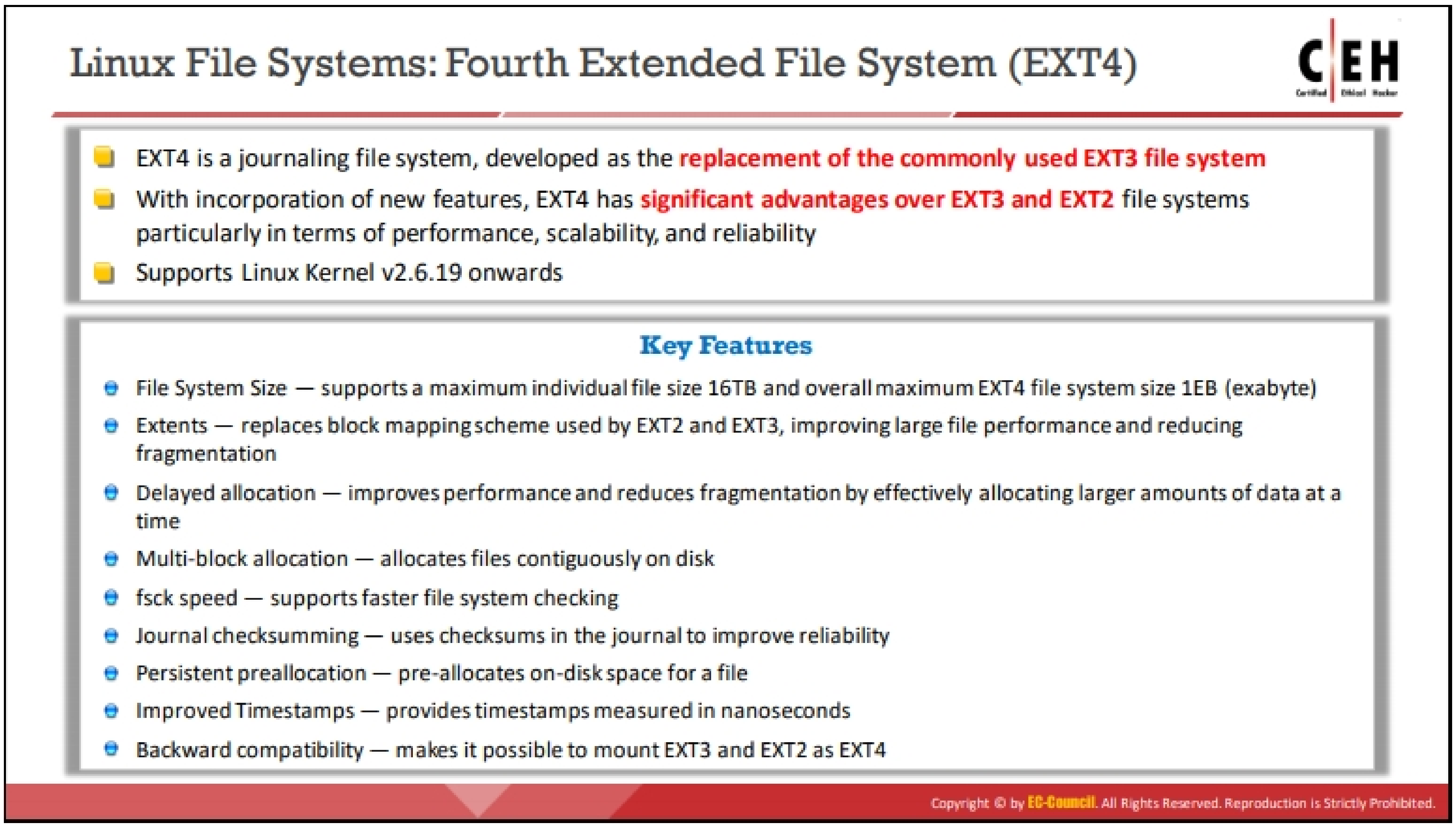
Speed

- As the EXT3 file system is journaling the file system, it has **higher throughput**, in most cases, than EXT2

Easy Transition

- The user can easily change the file system from EXT2 to EXT3 and **increase the performance** of the system

Notes: ____

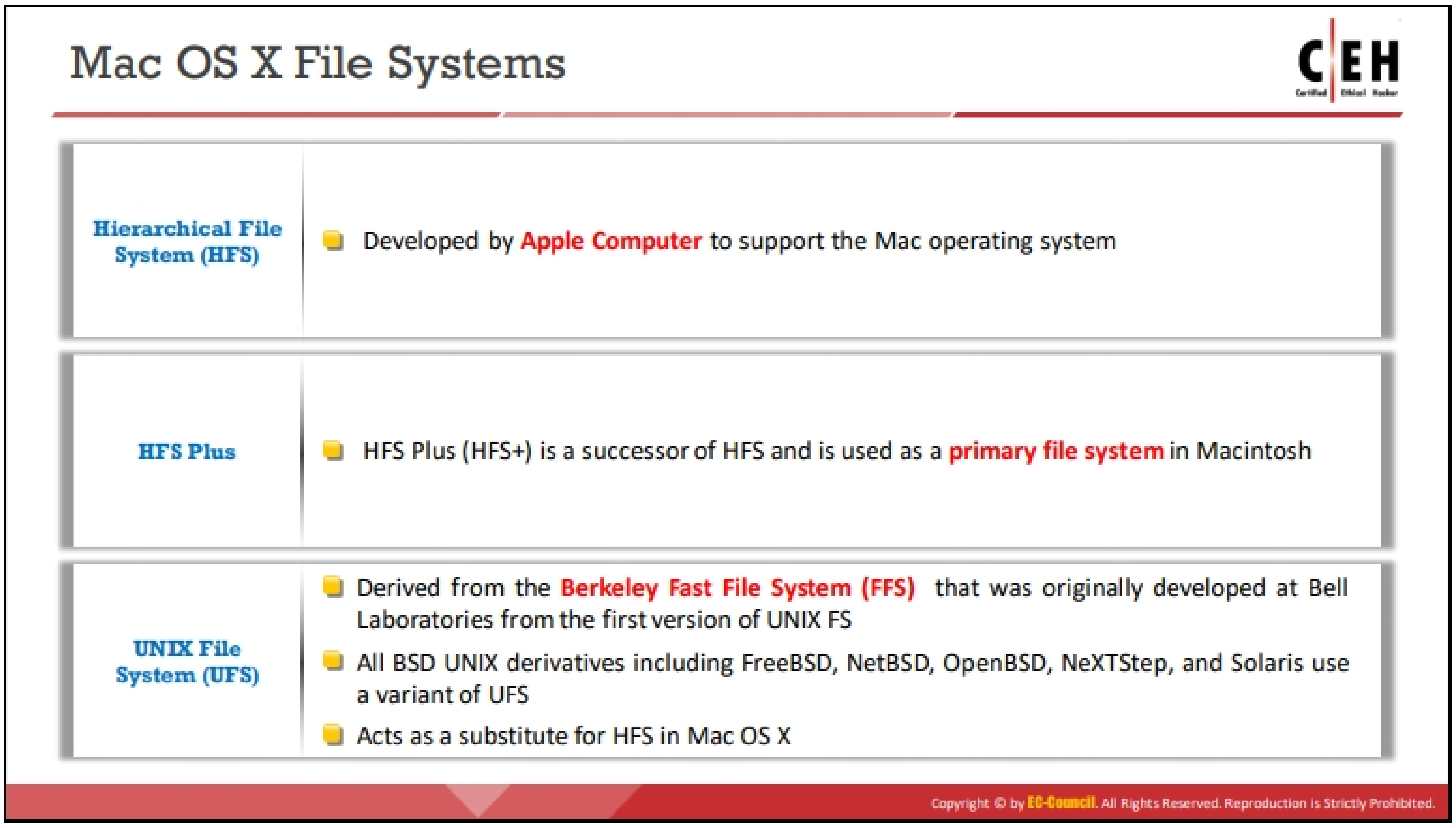


Linux File Systems: Fourth Extended File System (EXT4)

- EXT4 is a journaling file system, developed as the **replacement of the commonly used EXT3 file system**
- With incorporation of new features, EXT4 has **significant advantages over EXT3 and EXT2** file systems particularly in terms of performance, scalability, and reliability
- Supports Linux Kernel v2.6.19 onwards

Key Features

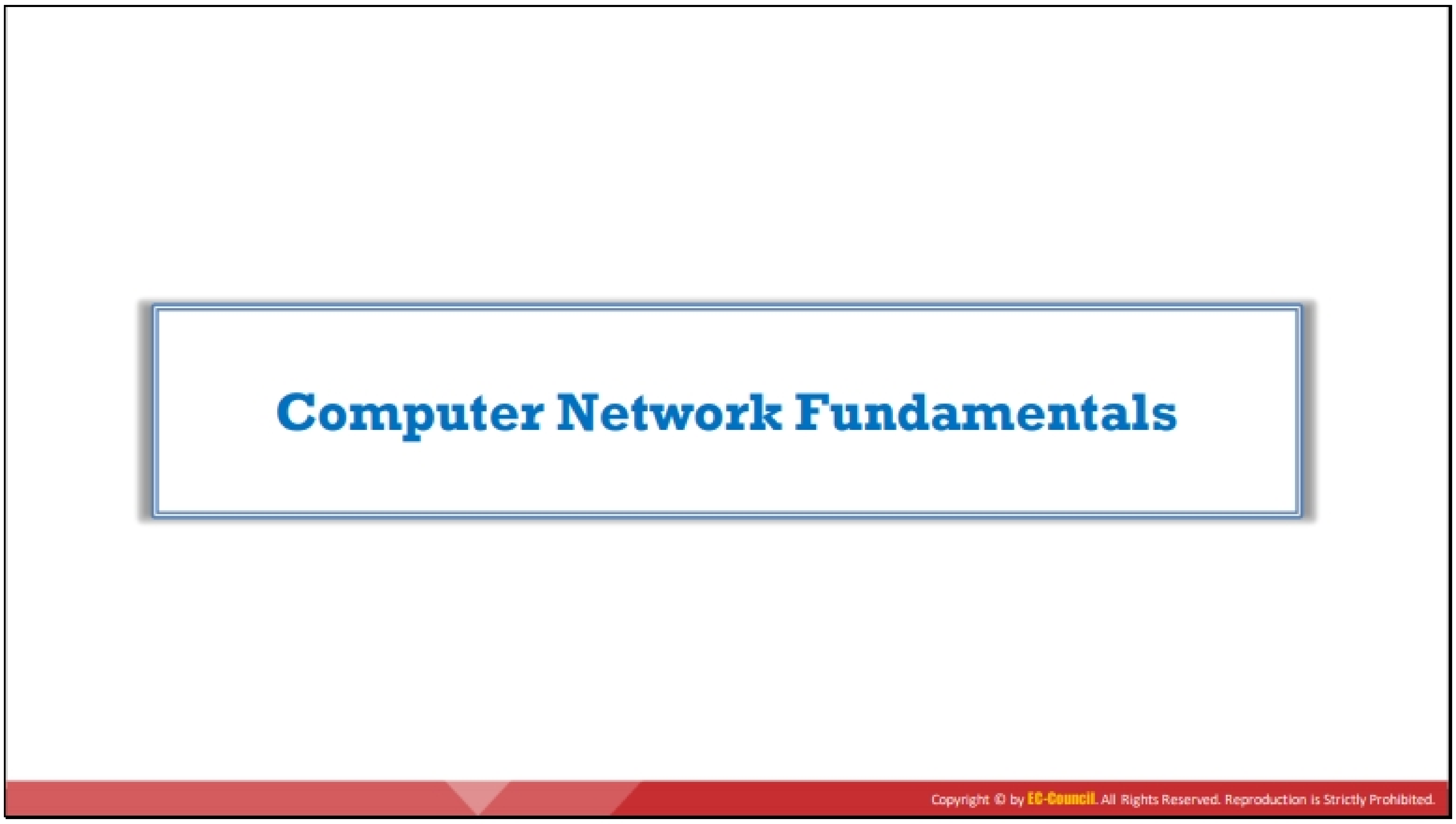
- File System Size — supports a maximum individual file size 16TB and overall maximum EXT4 file system size 1EB (exabyte)
- Extents — replaces block mapping scheme used by EXT2 and EXT3, improving large file performance and reducing fragmentation
- Delayed allocation — improves performance and reduces fragmentation by effectively allocating larger amounts of data at a time
- Multi-block allocation — allocates files contiguously on disk
- fsck speed — supports faster file system checking
- Journal checksumming — uses checksums in the journal to improve reliability
- Persistent preallocation — pre-allocates on-disk space for a file
- Improved Timestamps — provides timestamps measured in nanoseconds
- Backward compatibility — makes it possible to mount EXT3 and EXT2 as EXT4



Mac OS X File Systems

Hierarchical File System (HFS)	Developed by **Apple Computer** to support the Mac operating system
HFS Plus	HFS Plus (HFS+) is a successor of HFS and is used as a **primary file system** in Macintosh
UNIX File System (UFS)	Derived from the **Berkeley Fast File System (FFS)** that was originally developed at Bell Laboratories from the first version of UNIX FS All BSD UNIX derivatives including FreeBSD, NetBSD, OpenBSD, NeXTStep, and Solaris use a variant of UFS Acts as a substitute for HFS in Mac OS X

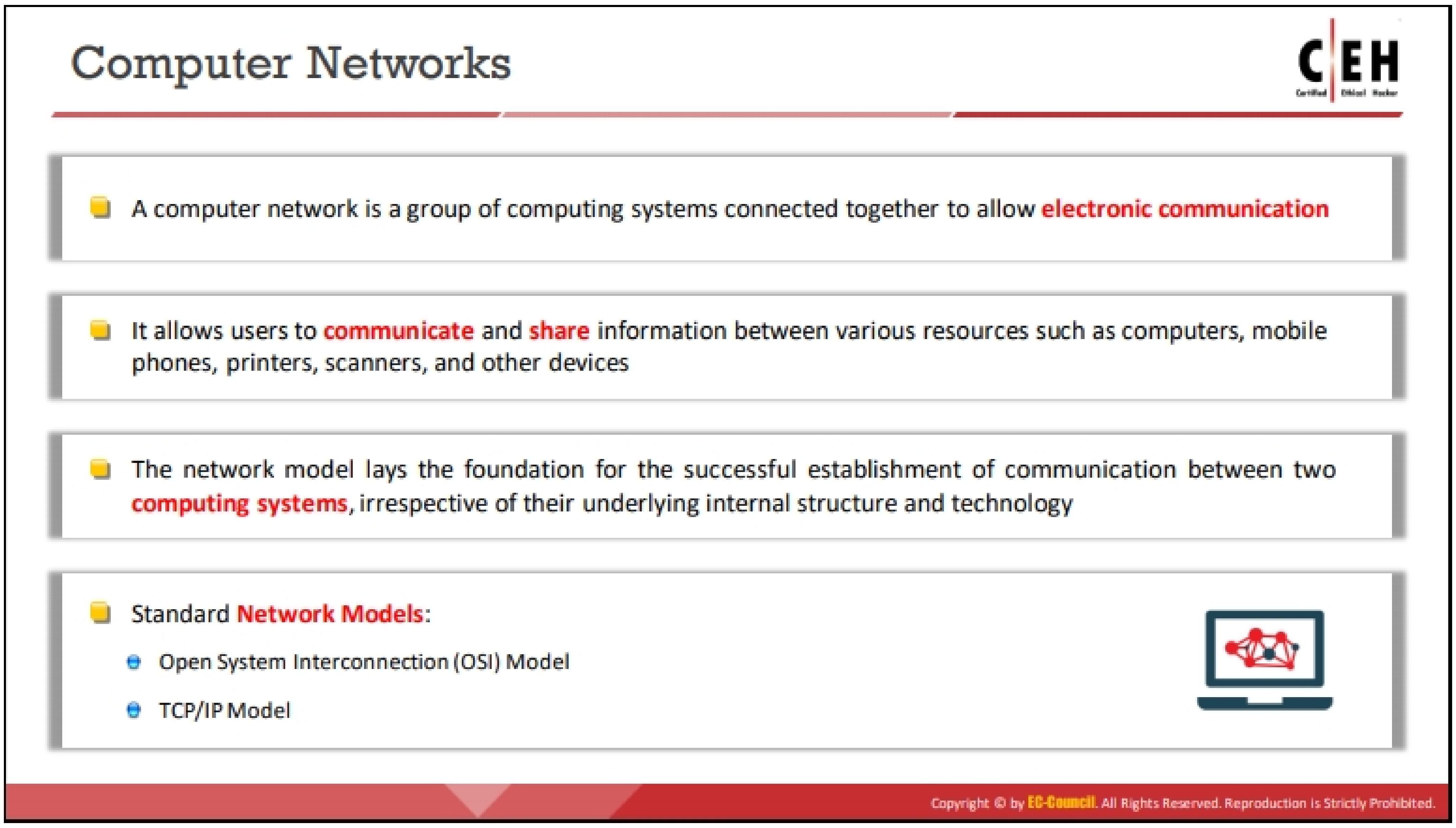
Notes: ____________________



Computer Network Fundamentals

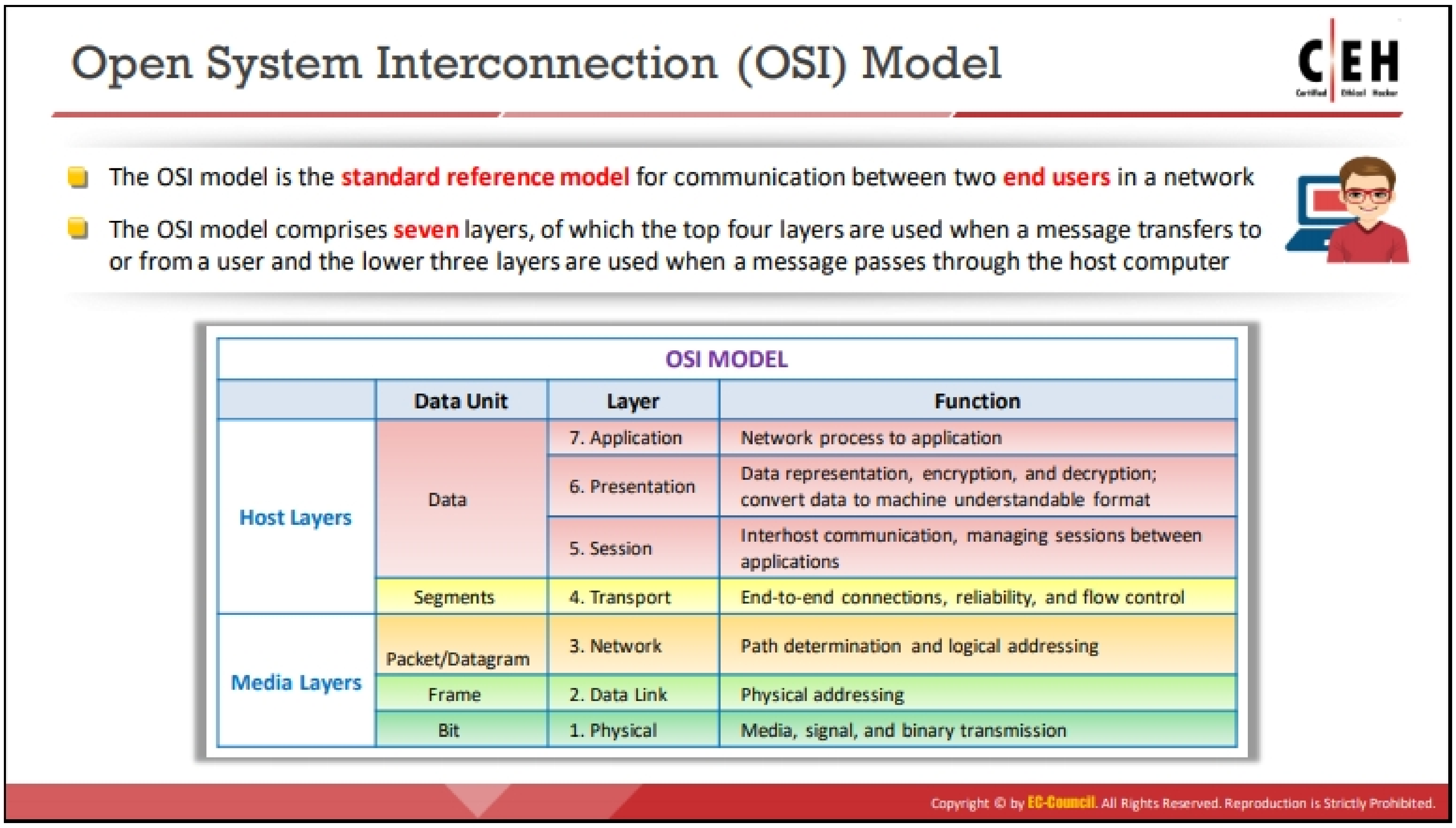
Computer Networks

Notes:



Computer Networks

- A computer network is a group of computing systems connected together to allow **electronic communication**
- It allows users to **communicate** and **share** information between various resources such as computers, mobile phones, printers, scanners, and other devices
- The network model lays the foundation for the successful establishment of communication between two **computing systems**, irrespective of their underlying internal structure and technology
- Standard **Network Models**:
  - Open System Interconnection (OSI) Model
  - TCP/IP Model



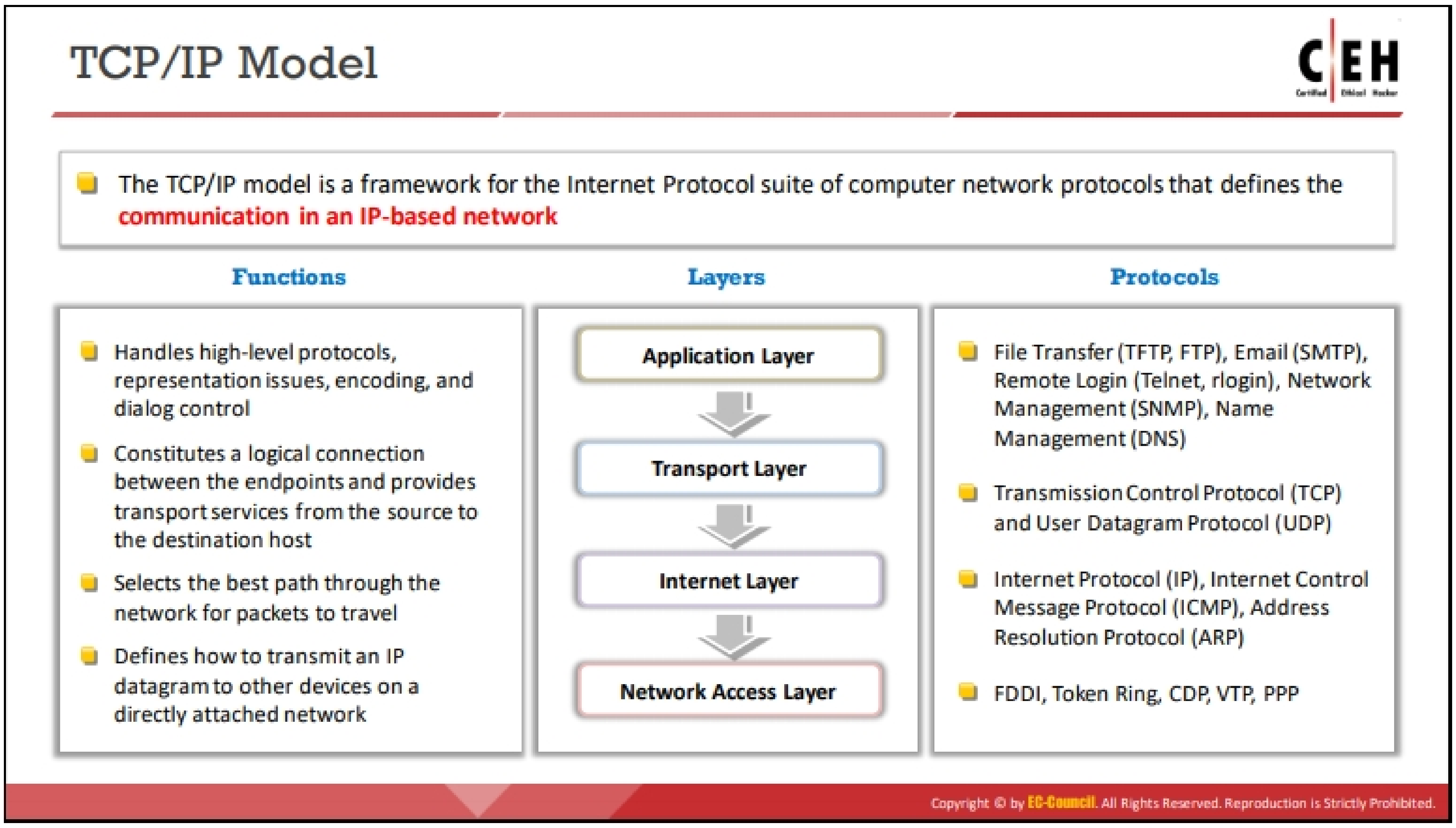
Open System Interconnection (OSI) Model

- The OSI model is the **standard reference model** for communication between two **end users** in a network
- The OSI model comprises **seven** layers, of which the top four layers are used when a message transfers to or from a user and the lower three layers are used when a message passes through the host computer

OSI MODEL

	Data Unit	Layer	Function
Host Layers	Data	7. Application	Network process to application
		6. Presentation	Data representation, encryption, and decryption; convert data to machine understandable format
		5. Session	Interhost communication, managing sessions between applications
	Segments	4. Transport	End-to-end connections, reliability, and flow control
Media Layers	Packet/Datagram	3. Network	Path determination and logical addressing
	Frame	2. Data Link	Physical addressing
	Bit	1. Physical	Media, signal, and binary transmission

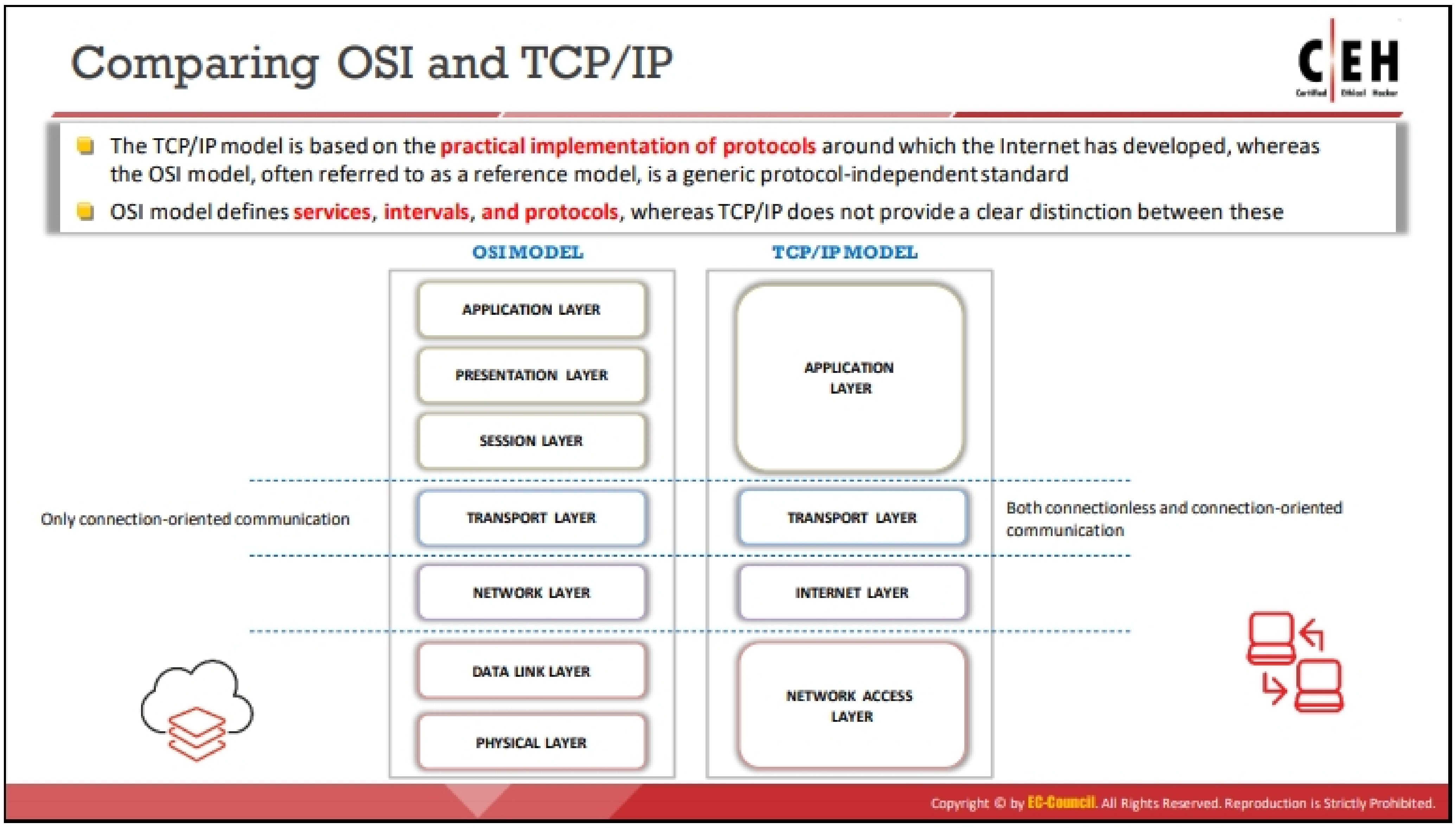
Notes:



TCP/IP Model

- The TCP/IP model is a framework for the Internet Protocol suite of computer network protocols that defines the **communication in an IP-based network**

Functions	Layers	Protocols
Handles high-level protocols, representation issues, encoding, and dialog control	**Application Layer**	File Transfer (TFTP, FTP), Email (SMTP), Remote Login (Telnet, rlogin), Network Management (SNMP), Name Management (DNS)
Constitutes a logical connection between the endpoints and provides transport services from the source to the destination host	**Transport Layer**	Transmission Control Protocol (TCP) and User Datagram Protocol (UDP)
Selects the best path through the network for packets to travel	**Internet Layer**	Internet Protocol (IP), Internet Control Message Protocol (ICMP), Address Resolution Protocol (ARP)
Defines how to transmit an IP datagram to other devices on a directly attached network	**Network Access Layer**	FDDI, Token Ring, CDP, VTP, PPP

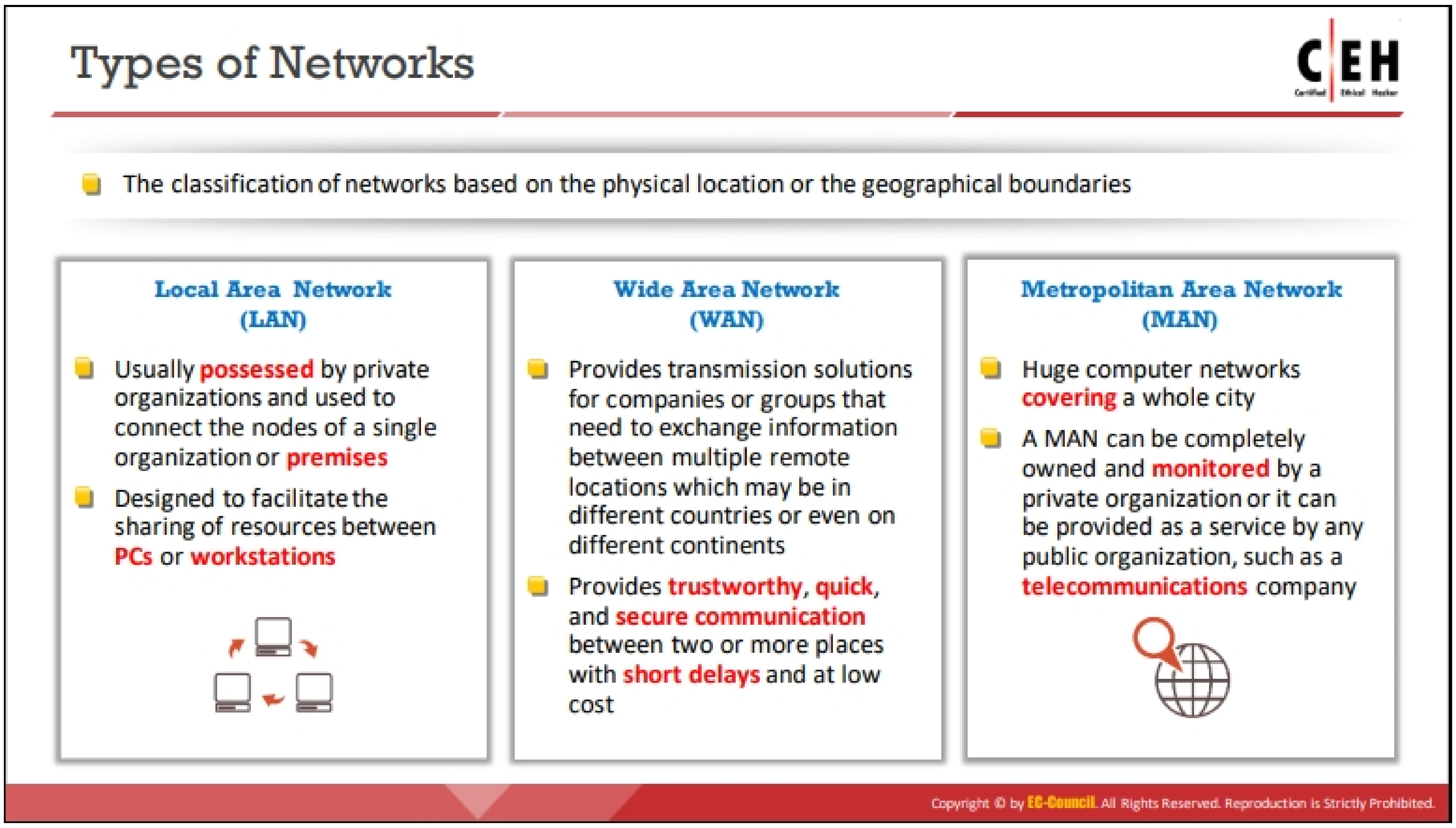


Comparing OSI and TCP/IP

- The TCP/IP model is based on the **practical implementation of protocols** around which the Internet has developed, whereas the OSI model, often referred to as a reference model, is a generic protocol-independent standard
- OSI model defines **services**, **intervals**, **and protocols**, whereas TCP/IP does not provide a clear distinction between these

	OSI MODEL	TCP/IP MODEL	
	APPLICATION LAYER	APPLICATION LAYER	
	PRESENTATION LAYER		
	SESSION LAYER		
Only connection-oriented communication	TRANSPORT LAYER	TRANSPORT LAYER	Both connectionless and connection-oriented communication
	NETWORK LAYER	INTERNET LAYER	
	DATA LINK LAYER	NETWORK ACCESS LAYER	
	PHYSICAL LAYER		

Notes:



Types of Networks

- The classification of networks based on the physical location or the geographical boundaries

Local Area Network (LAN)

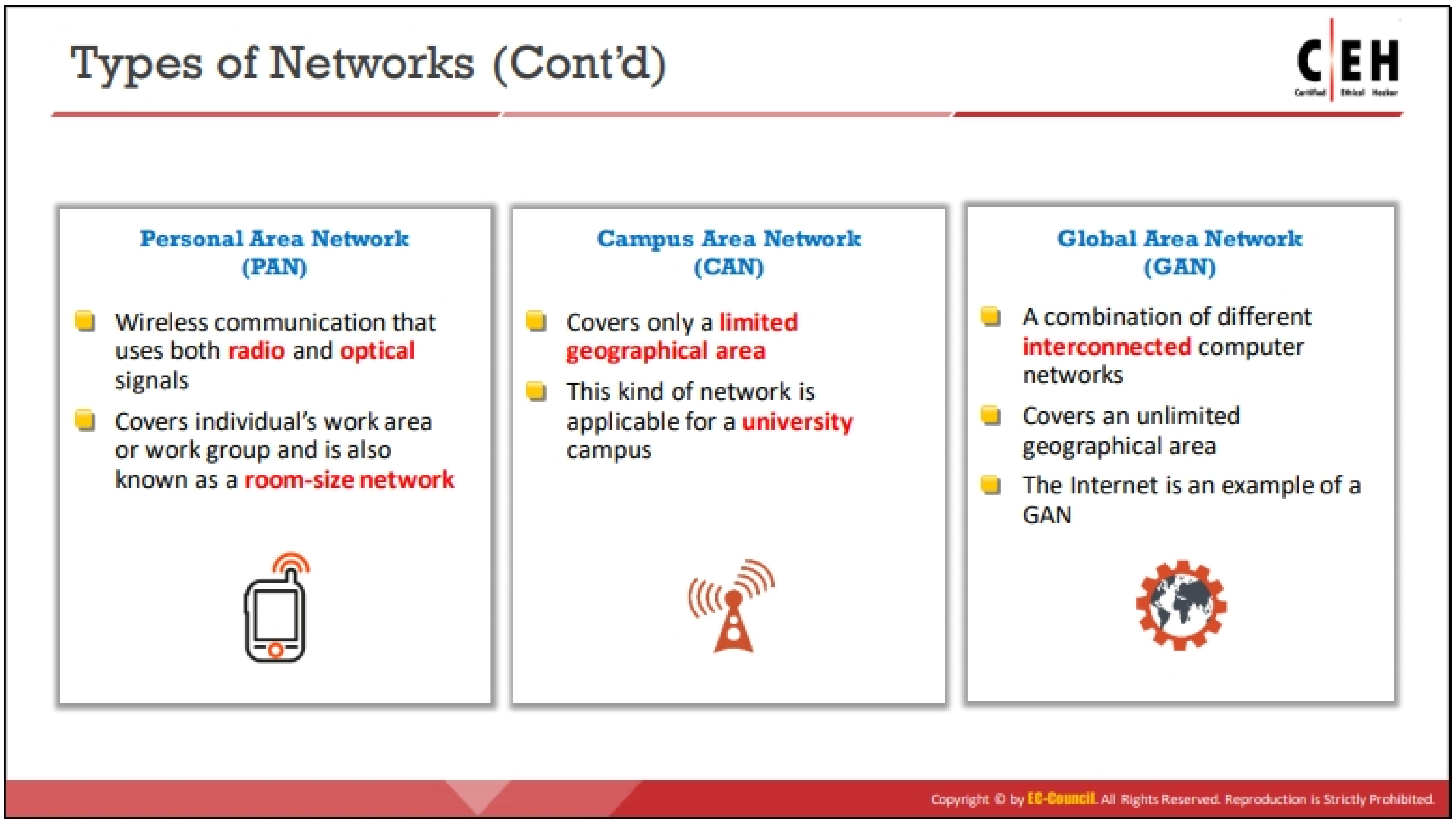
- Usually possessed by private organizations and used to connect the nodes of a single organization or premises
- Designed to facilitate the sharing of resources between PCs or workstations

Wide Area Network (WAN)

- Provides transmission solutions for companies or groups that need to exchange information between multiple remote locations which may be in different countries or even on different continents
- Provides trustworthy, quick, and secure communication between two or more places with short delays and at low cost

Metropolitan Area Network (MAN)

- Huge computer networks covering a whole city
- A MAN can be completely owned and monitored by a private organization or it can be provided as a service by any public organization, such as a telecommunications company



Types of Networks (Cont'd)

Personal Area Network (PAN)

- Wireless communication that uses both radio and optical signals
- Covers individual's work area or work group and is also known as a room-size network

Campus Area Network (CAN)

- Covers only a limited geographical area
- This kind of network is applicable for a university campus

Global Area Network (GAN)

- A combination of different interconnected computer networks
- Covers an unlimited geographical area
- The Internet is an example of a GAN

Notes: ____

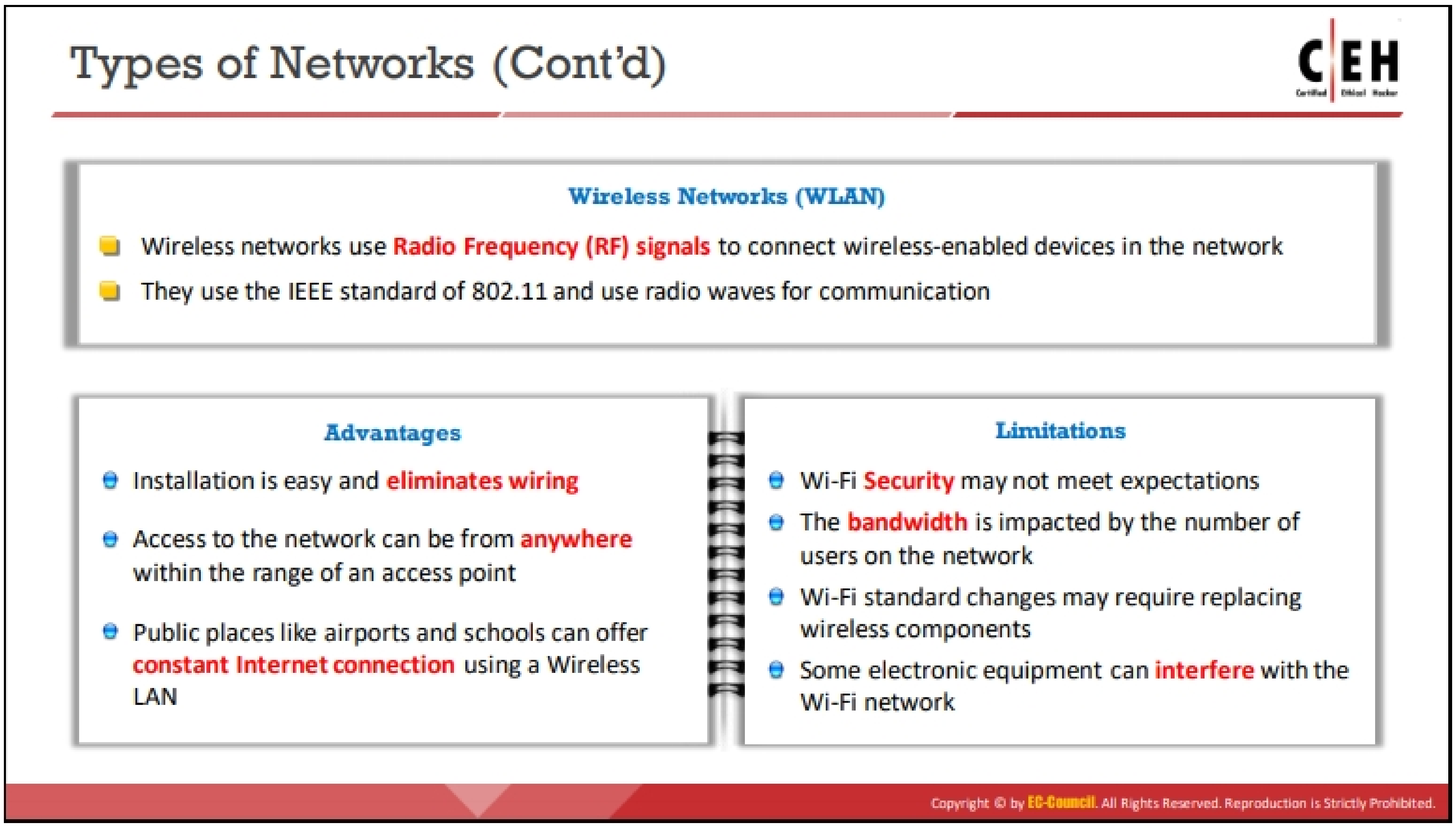
____

____

____

____

____



Types of Networks (Cont'd)

Wireless Networks (WLAN)

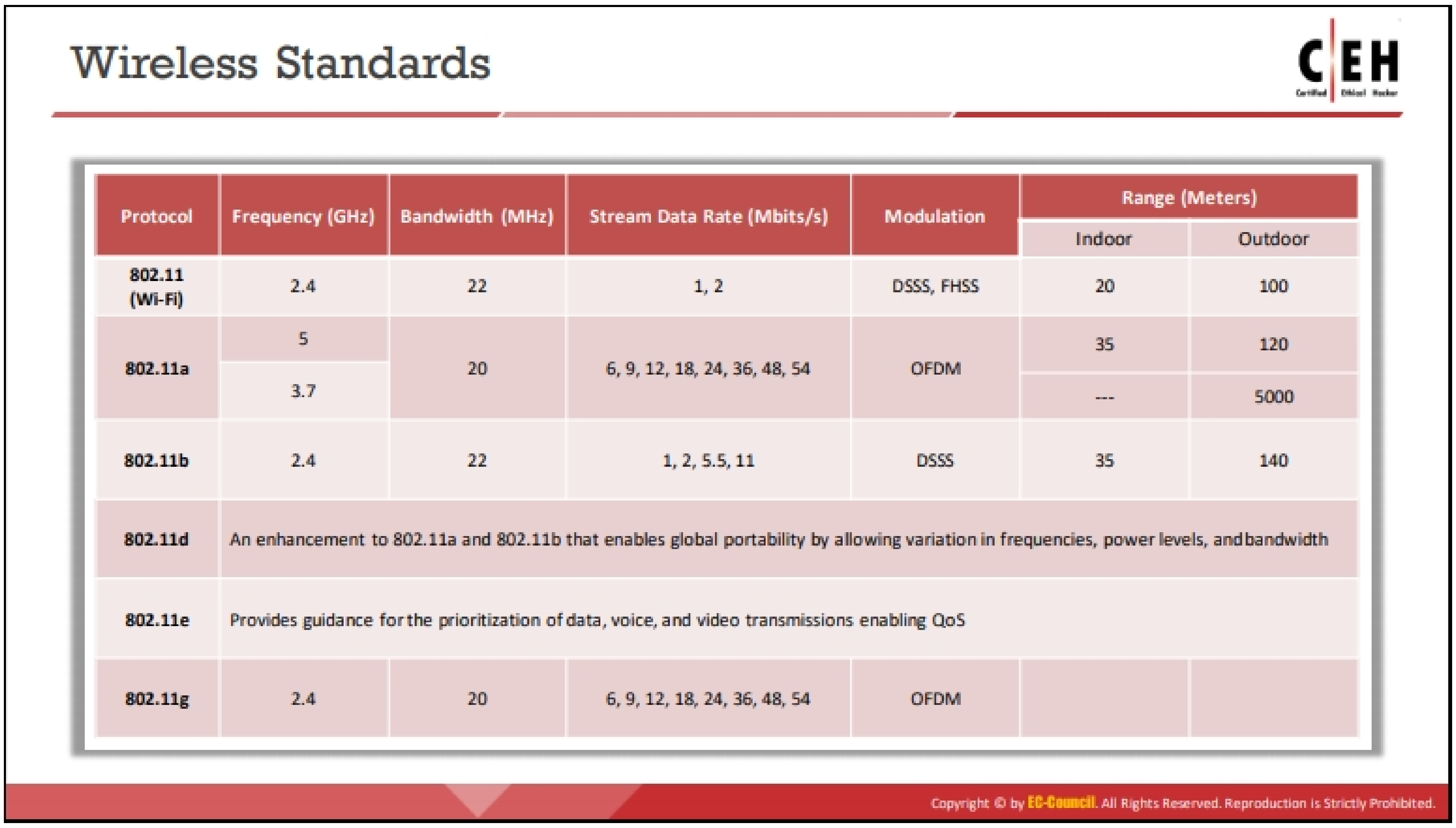
- Wireless networks use **Radio Frequency (RF) signals** to connect wireless-enabled devices in the network
- They use the IEEE standard of 802.11 and use radio waves for communication

Advantages

- Installation is easy and **eliminates wiring**
- Access to the network can be from **anywhere** within the range of an access point
- Public places like airports and schools can offer **constant Internet connection** using a Wireless LAN

Limitations

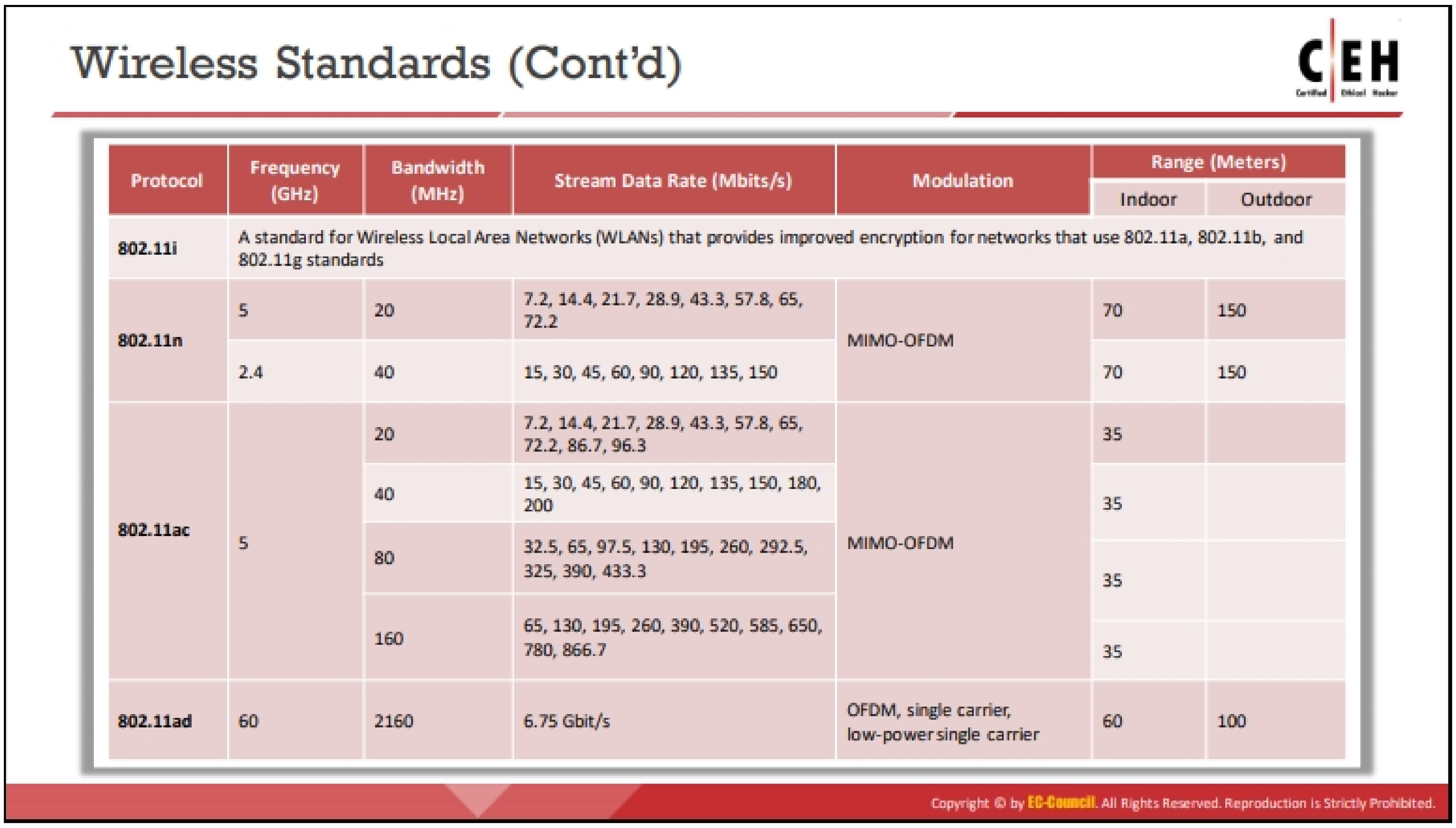
- Wi-Fi **Security** may not meet expectations
- The **bandwidth** is impacted by the number of users on the network
- Wi-Fi standard changes may require replacing wireless components
- Some electronic equipment can **interfere** with the Wi-Fi network



Wireless Standards

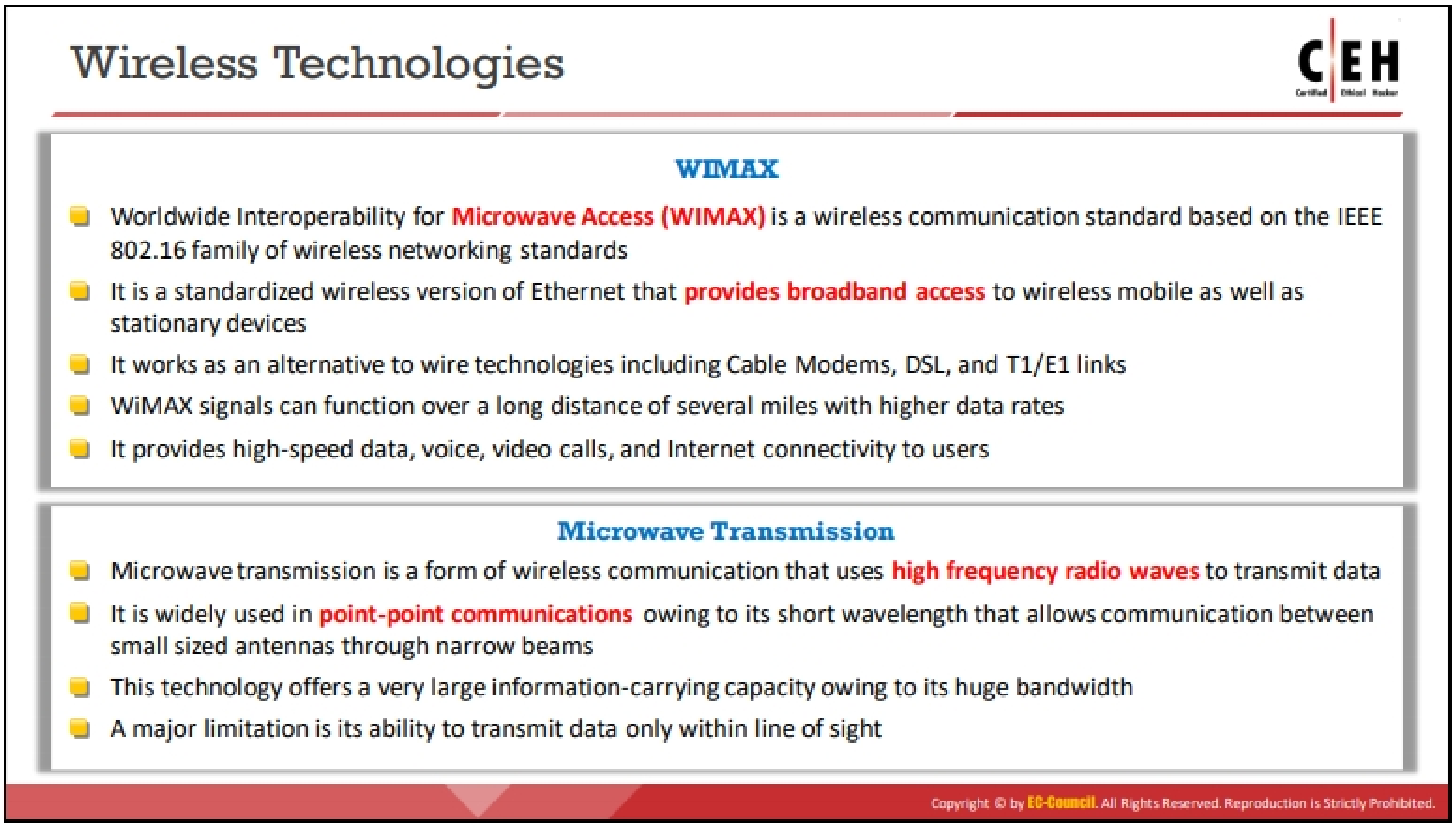
Protocol	Frequency (GHz)	Bandwidth (MHz)	Stream Data Rate (Mbits/s)	Modulation	Range (Meters)	
					Indoor	Outdoor
802.11 (Wi-Fi)	2.4	22	1, 2	DSSS, FHSS	20	100
802.11a	5	20	6, 9, 12, 18, 24, 36, 48, 54	OFDM	35	120
	3.7				---	5000
802.11b	2.4	22	1, 2, 5.5, 11	DSSS	35	140
802.11d	An enhancement to 802.11a and 802.11b that enables global portability by allowing variation in frequencies, power levels, and bandwidth					
802.11e	Provides guidance for the prioritization of data, voice, and video transmissions enabling QoS					
802.11g	2.4	20	6, 9, 12, 18, 24, 36, 48, 54	OFDM		

Notes:



Wireless Standards (Cont'd)

Protocol	Frequency (GHz)	Bandwidth (MHz)	Stream Data Rate (Mbits/s)	Modulation	Range (Meters)	
					Indoor	Outdoor
802.11i	A standard for Wireless Local Area Networks (WLANs) that provides improved encryption for networks that use 802.11a, 802.11b, and 802.11g standards					
802.11n	5	20	7.2, 14.4, 21.7, 28.9, 43.3, 57.8, 65, 72.2	MIMO-OFDM	70	150
	2.4	40	15, 30, 45, 60, 90, 120, 135, 150		70	150
802.11ac	5	20	7.2, 14.4, 21.7, 28.9, 43.3, 57.8, 65, 72.2, 86.7, 96.3	MIMO-OFDM	35	
		40	15, 30, 45, 60, 90, 120, 135, 150, 180, 200		35	
		80	32.5, 65, 97.5, 130, 195, 260, 292.5, 325, 390, 433.3		35	
		160	65, 130, 195, 260, 390, 520, 585, 650, 780, 866.7		35	
802.11ad	60	2160	6.75 Gbit/s	OFDM, single carrier, low-power single carrier	60	100



Wireless Technologies

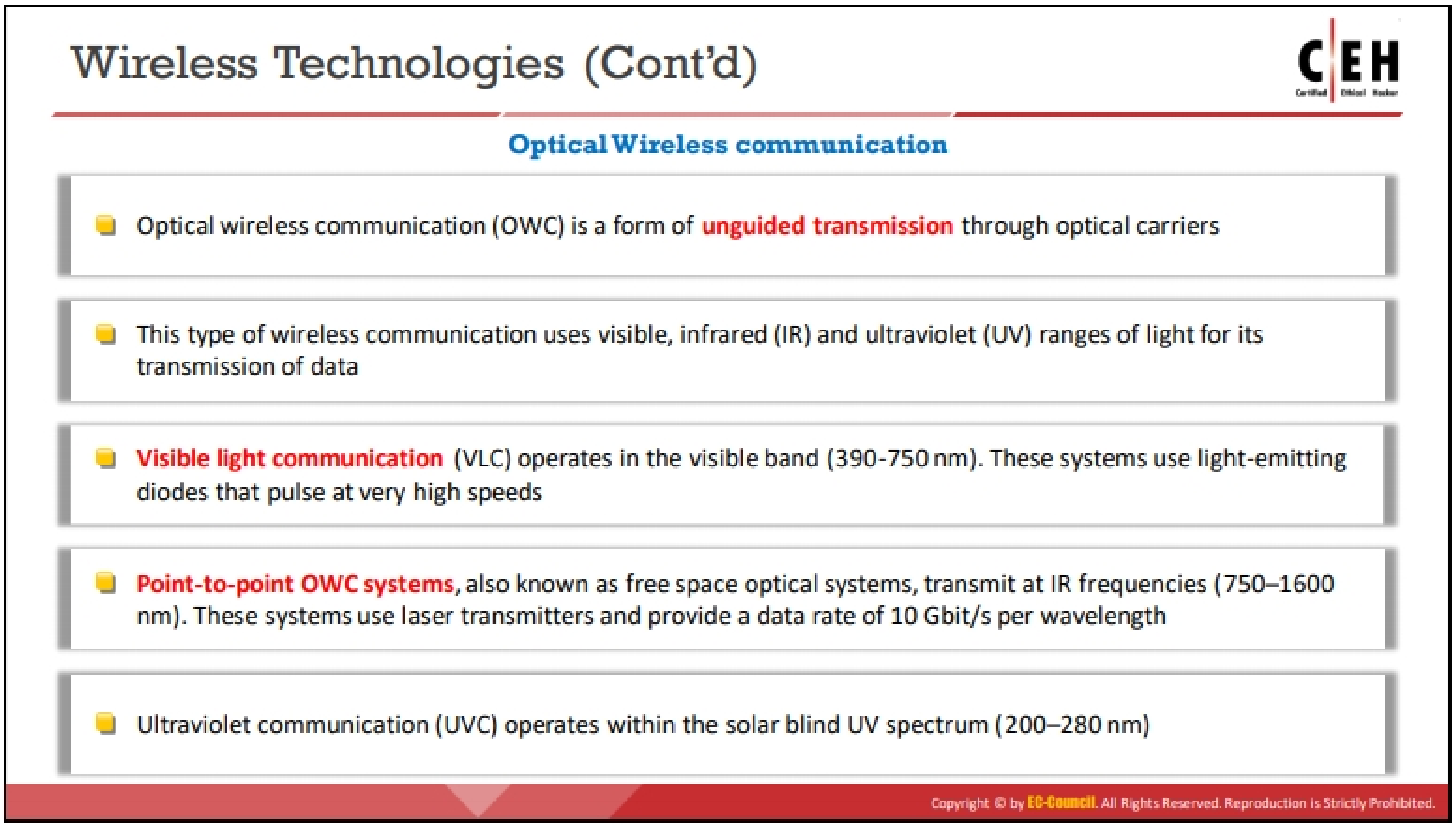
WIMAX

- Worldwide Interoperability for **Microwave Access (WIMAX)** is a wireless communication standard based on the IEEE 802.16 family of wireless networking standards
- It is a standardized wireless version of Ethernet that **provides broadband access** to wireless mobile as well as stationary devices
- It works as an alternative to wire technologies including Cable Modems, DSL, and T1/E1 links
- WiMAX signals can function over a long distance of several miles with higher data rates
- It provides high-speed data, voice, video calls, and Internet connectivity to users

Microwave Transmission

- Microwave transmission is a form of wireless communication that uses **high frequency radio waves** to transmit data
- It is widely used in **point-point communications** owing to its short wavelength that allows communication between small sized antennas through narrow beams
- This technology offers a very large information-carrying capacity owing to its huge bandwidth
- A major limitation is its ability to transmit data only within line of sight

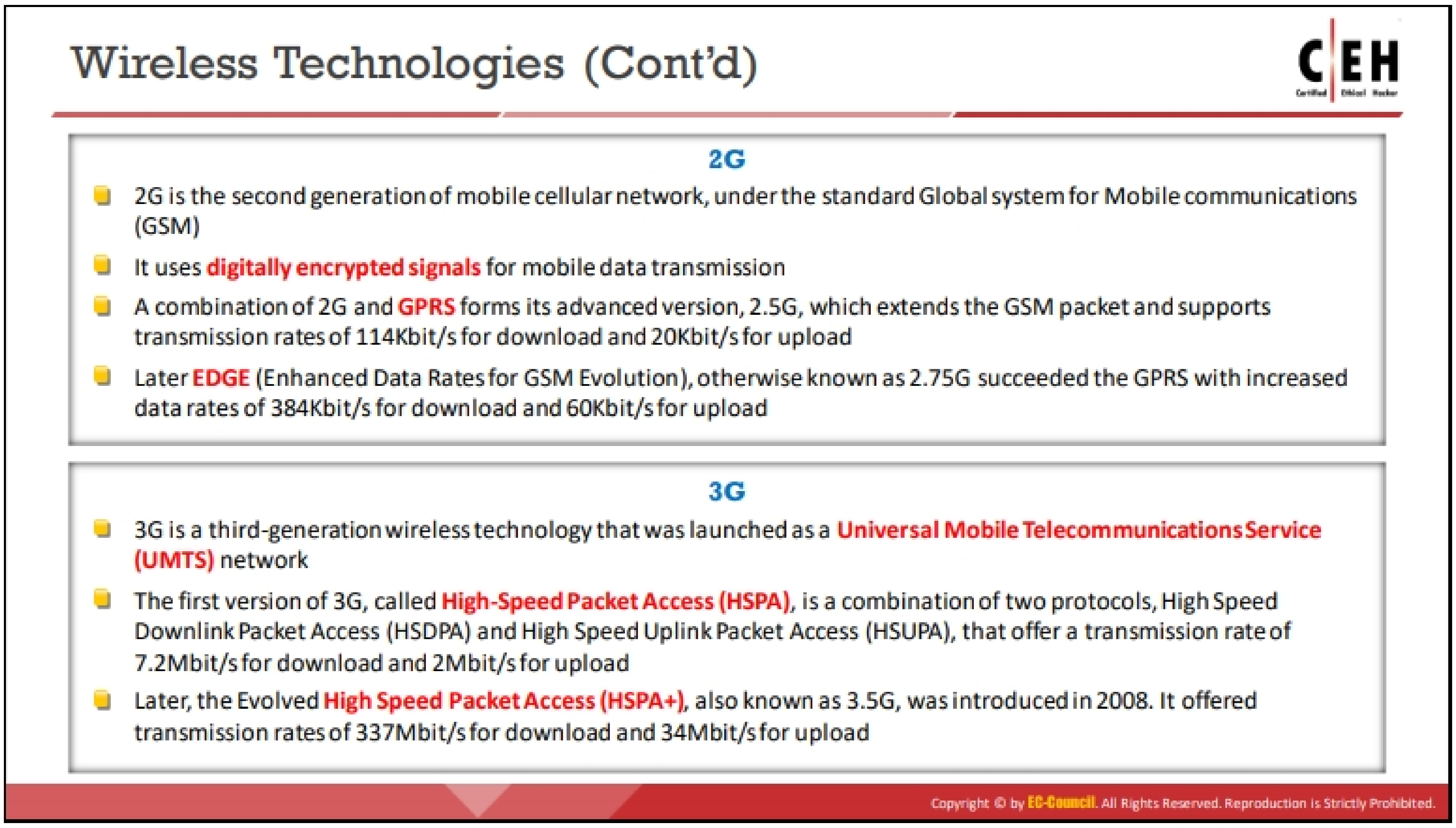
Notes:



Wireless Technologies (Cont'd)

Optical Wireless communication

- Optical wireless communication (OWC) is a form of **unguided transmission** through optical carriers
- This type of wireless communication uses visible, infrared (IR) and ultraviolet (UV) ranges of light for its transmission of data
- **Visible light communication** (VLC) operates in the visible band (390-750 nm). These systems use light-emitting diodes that pulse at very high speeds
- **Point-to-point OWC systems**, also known as free space optical systems, transmit at IR frequencies (750–1600 nm). These systems use laser transmitters and provide a data rate of 10 Gbit/s per wavelength
- Ultraviolet communication (UVC) operates within the solar blind UV spectrum (200–280 nm)



Wireless Technologies (Cont'd)

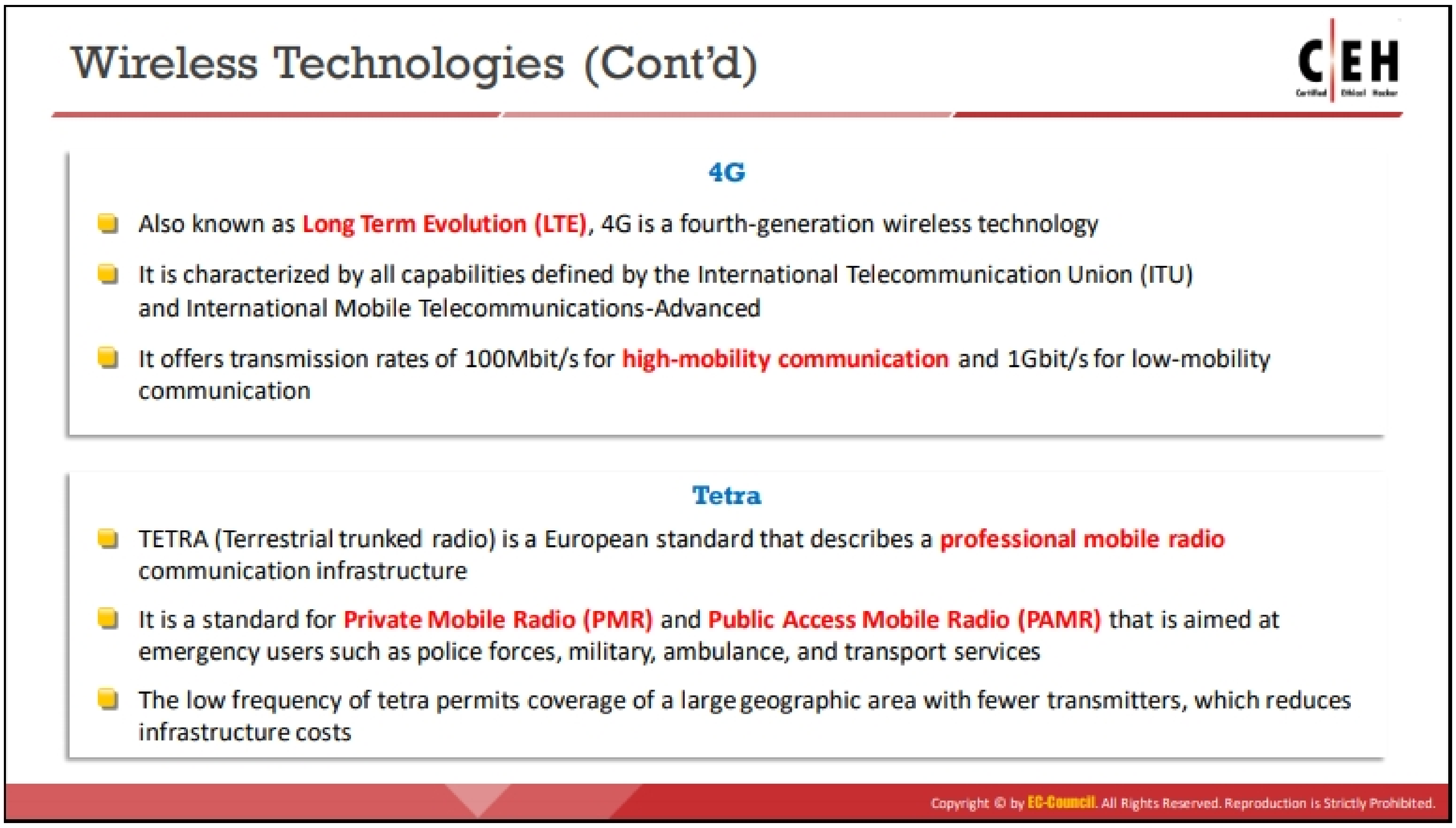
2G

- 2G is the second generation of mobile cellular network, under the standard Global system for Mobile communications (GSM)
- It uses **digitally encrypted signals** for mobile data transmission
- A combination of 2G and **GPRS** forms its advanced version, 2.5G, which extends the GSM packet and supports transmission rates of 114Kbit/s for download and 20Kbit/s for upload
- Later **EDGE** (Enhanced Data Rates for GSM Evolution), otherwise known as 2.75G succeeded the GPRS with increased data rates of 384Kbit/s for download and 60Kbit/s for upload

3G

- 3G is a third-generation wireless technology that was launched as a **Universal Mobile Telecommunications Service (UMTS)** network
- The first version of 3G, called **High-Speed Packet Access (HSPA)**, is a combination of two protocols, High Speed Downlink Packet Access (HSDPA) and High Speed Uplink Packet Access (HSUPA), that offer a transmission rate of 7.2Mbit/s for download and 2Mbit/s for upload
- Later, the Evolved **High Speed Packet Access (HSPA+)**, also known as 3.5G, was introduced in 2008. It offered transmission rates of 337Mbit/s for download and 34Mbit/s for upload

Notes:



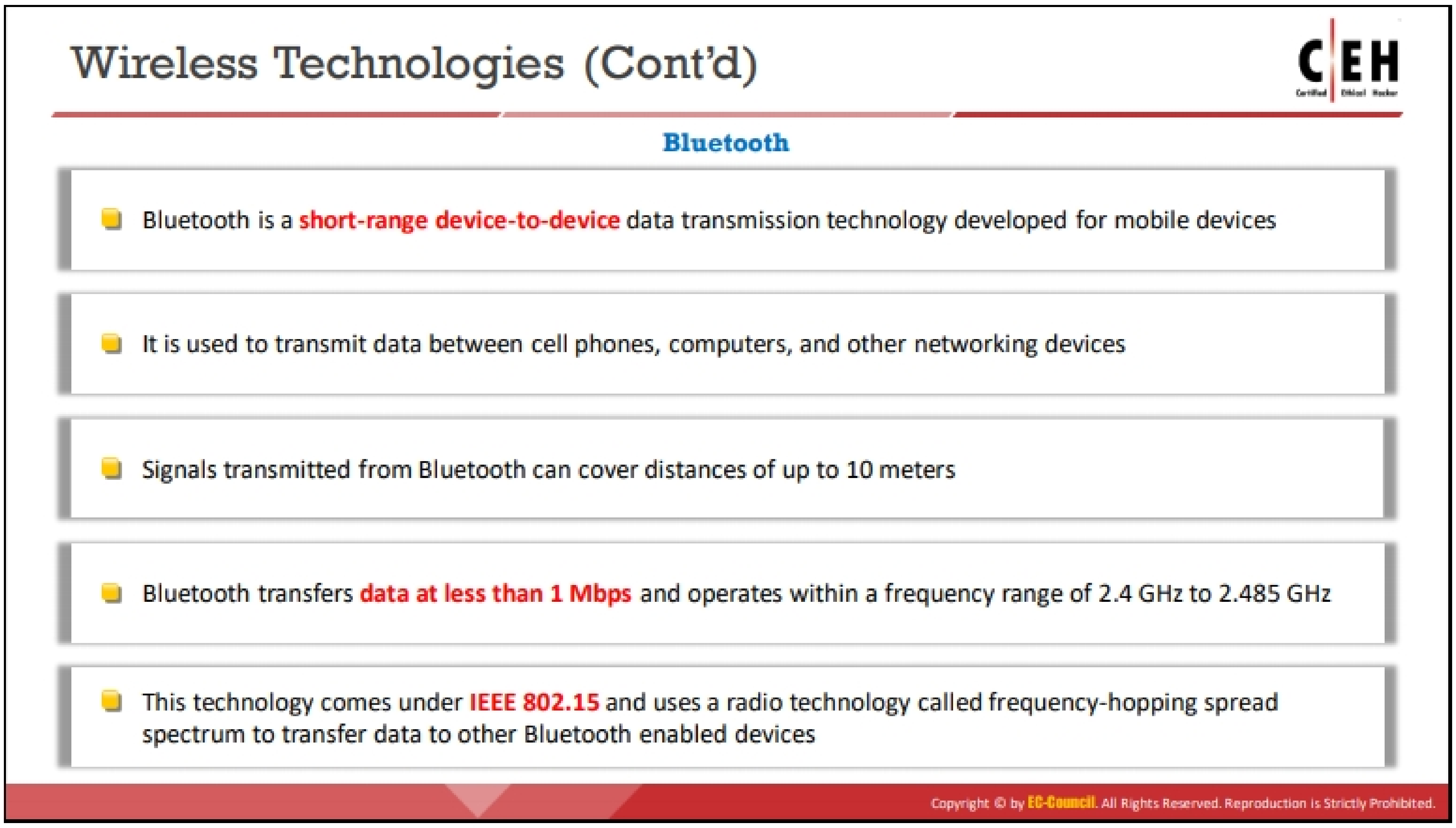
Wireless Technologies (Cont'd)

4G

- Also known as **Long Term Evolution (LTE)**, 4G is a fourth-generation wireless technology
- It is characterized by all capabilities defined by the International Telecommunication Union (ITU) and International Mobile Telecommunications-Advanced
- It offers transmission rates of 100Mbit/s for **high-mobility communication** and 1Gbit/s for low-mobility communication

Tetra

- TETRA (Terrestrial trunked radio) is a European standard that describes a **professional mobile radio** communication infrastructure
- It is a standard for **Private Mobile Radio (PMR)** and **Public Access Mobile Radio (PAMR)** that is aimed at emergency users such as police forces, military, ambulance, and transport services
- The low frequency of tetra permits coverage of a large geographic area with fewer transmitters, which reduces infrastructure costs



Wireless Technologies (Cont'd)

Bluetooth

- Bluetooth is a **short-range device-to-device** data transmission technology developed for mobile devices
- It is used to transmit data between cell phones, computers, and other networking devices
- Signals transmitted from Bluetooth can cover distances of up to 10 meters
- Bluetooth transfers **data at less than 1 Mbps** and operates within a frequency range of 2.4 GHz to 2.485 GHz
- This technology comes under **IEEE 802.15** and uses a radio technology called frequency-hopping spread spectrum to transfer data to other Bluetooth enabled devices

Notes:

Network Topologies

- Network topology is a specification that **deals with a network's overall design and flow of its data**

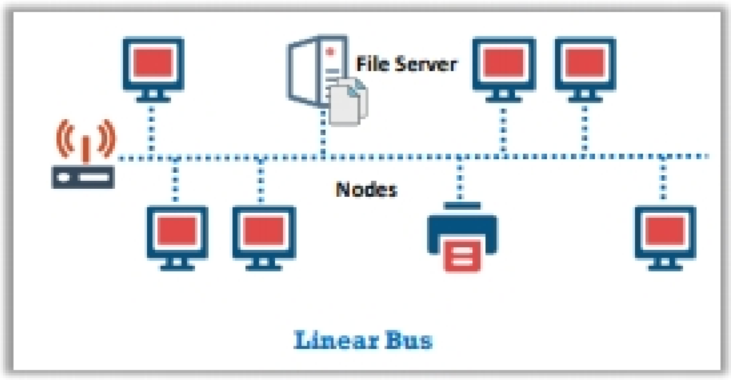
Types of Topology

- **Physical Topology** – The physical layout of nodes, workstations and cables in the network
- **Logical Topology** – The information flow between different components

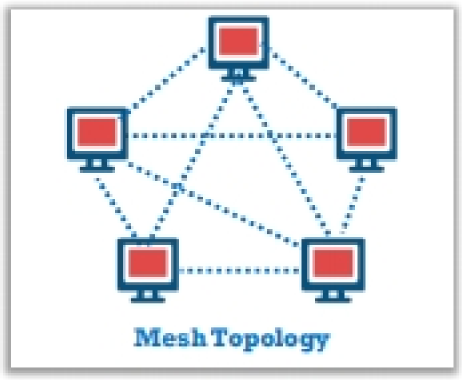
Physical Network Topologies

Bus Topology	**Star Topology**
Network devices are connected to the central cable, called a bus, using interface connectors	Network devices are connected to a central computer called a hub which functions as a router to send messages
Ring Topology	**Mesh Topology**
Network devices are connected in a closed loop. Data travels from node to node, with each node handling every packet along the way	Network devices are connected in such a way that every device has a point-to-point link with every other device on the network
Tree Topology	**Hybrid Topology**
A hybrid of bus and star topologies, in which groups of star-configured networks are connected to a linear bus backbone cable	A combination of any two or more different topologies. Star-Bus or Star-Ring topologies are widely used

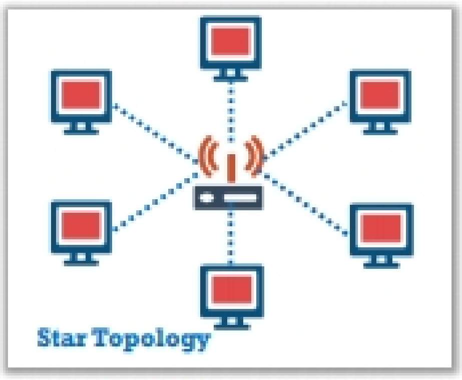
Network Topologies (Cont'd)



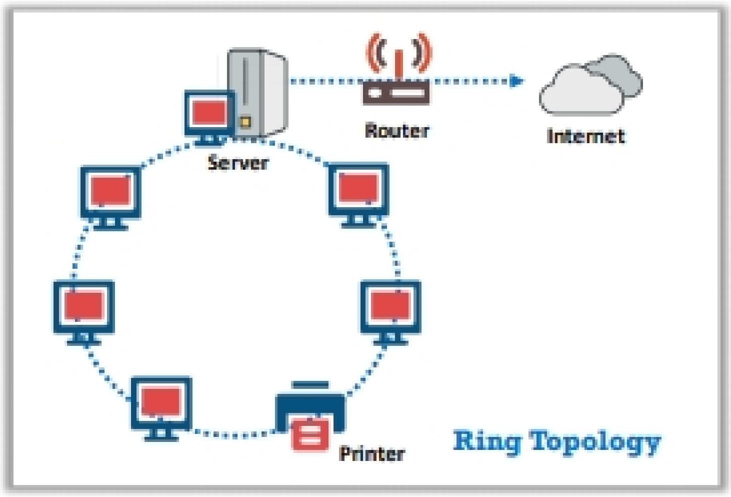
Linear Bus



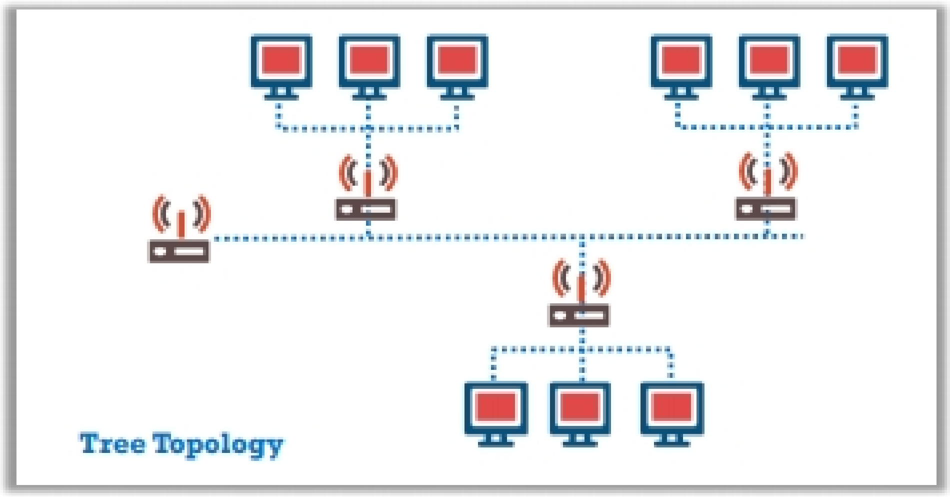
Mesh Topology



Star Topology



Ring Topology



Tree Topology

Notes: ____

____

____

____

____

____

Network Hardware Components

Network Interface Card (NIC)	Allows the computers to connect and communicate with the network
Repeater	Used to increase the strength of an incoming signal in a network
Hub	Used to connect segments of a LAN. All the LAN segments can see all the packets
Switch	Is similar to a hub. However, packets are not visible to any equipment in the LAN segment except the target node
Router	Receives data packets from one network segment and forwards them to another
Bridges	Combines two network segments and manages network traffic
Gateways	Enables communication between different types of environments and protocols

Types of LAN Technology

Ethernet

- Ethernet is the physical layer of LAN technology. It maintains proper balance between the speed, cost, and ease of installation
- It describes the number of conductors required for making the connection, determines the required performance thresholds, and offers the framework for data transmission
- A standard Ethernet network can send data at a rate of up to 10 Megabits per second (10 Mbps)
- Ethernet standard, IEEE standard 802.3, specifies configuration rules for an Ethernet network and also states the interaction of elements in a network

Fast Ethernet

- The Fast Ethernet standard, IEEE 802.3u, is a new version of ethernet that transmits data at a minimum rate of 100 Mbit/s
- Three types of Fast Ethernet are available in the market: 100BASE-TX , to use with level 5 UTP cable; 100BASE-FX, to use with a fiber-optic cable; and 100BASE-T4, for utilizing extra two wires with a level 3 UTP cable

Notes: ____

Types of LAN Technology (Cont'd)

Gigabit Ethernet

- Gigabit Ethernet was defined by the **IEEE 802.3-2008** standard and conveys Ethernet frames at a speed rate of a gigabit per second
- It is used on **fast speed communication** networks like multimedia and Voice over IP (VoIP)
- It is also called as "**Gigabit-Ethernet-over-copper**" or 1000Base-T, as its speed is ten times more than 100Base-T

10 Gigabit Ethernet

- 10 Gigabit Ethernet was first defined by the **IEEE 802.3ae-2002** standard
- It conveys Ethernet frames at a speed of **10 gigabits per second**. This makes it 10 times faster than Gigabit Ethernet
- Unlike other Ethernet systems, 10 Gigabit Ethernet uses optical fiber connections

Types of LAN Technology (Cont'd)

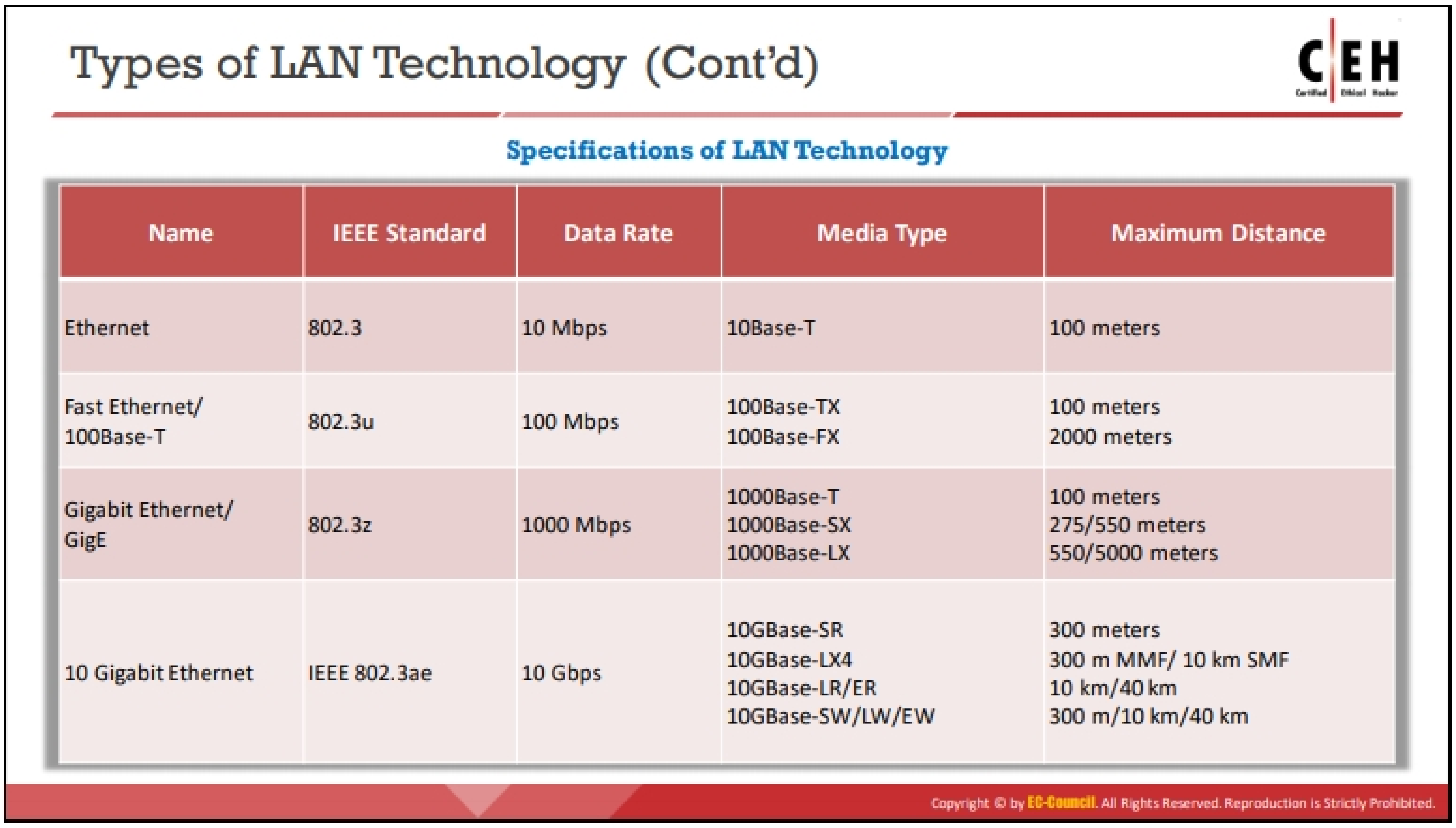
Asynchronous Transfer Mode (ATM)

- Asynchronous Transfer Mode (ATM) is a **cell-based fast-packet communication** standard developed for transmitting information of different types like voice, video or data, in small, and fixed-sized cells
- It operates on the **data link layer** through fiber or twisted-pair cable
- It is mainly used on **private long-distance networks**, especially by Internet service providers

Power over Ethernet (PoE)

- Power over Ethernet (PoE) is a networking feature defined by the **IEEE 802.3af** and **802.3at** standards
- It allows the Ethernet cables to supply power to network devices over the existing data connection
- PoE-capable devices can be power sourcing equipment (PSE), powered devices (PDs), and sometimes both. PSE is a device that transmits power, whereas PD is a device that is powered

Notes: ____



Types of LAN Technology (Cont'd)

Specifications of LAN Technology

Name	IEEE Standard	Data Rate	Media Type	Maximum Distance
Ethernet	802.3	10 Mbps	10Base-T	100 meters
Fast Ethernet/ 100Base-T	802.3u	100 Mbps	100Base-TX 100Base-FX	100 meters 2000 meters
Gigabit Ethernet/ GigE	802.3z	1000 Mbps	1000Base-T 1000Base-SX 1000Base-LX	100 meters 275/550 meters 550/5000 meters
10 Gigabit Ethernet	IEEE 802.3ae	10 Gbps	10GBase-SR 10GBase-LX4 10GBase-LR/ER 10GBase-SW/LW/EW	300 meters 300 m MMF/ 10 km SMF 10 km/40 km 300 m/10 km/40 km

Common Fiber Technologies

Notes:

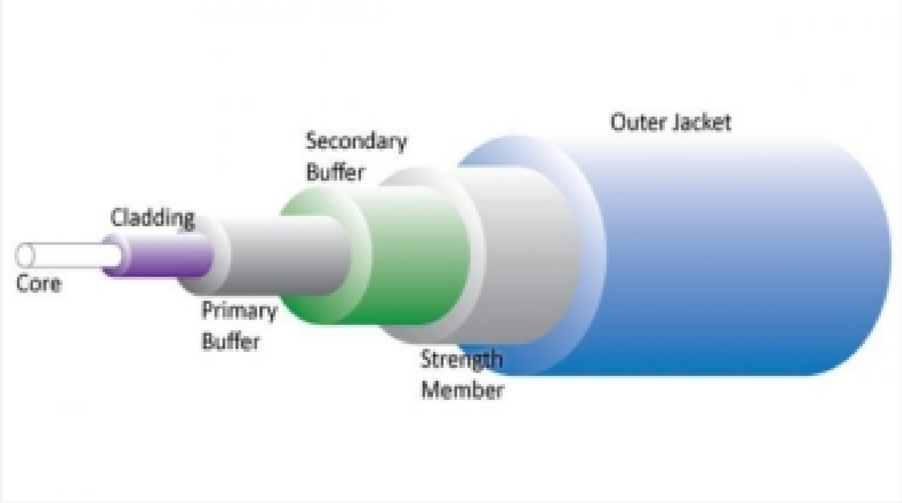
Types of Cables: Fiber Optic Cable

Fiber optic cable

- Optical fiber cable consists of the core, cladding, buffer, and jacket layers
- The core consists of glass or plastic with higher index of refraction than the cladding, and carries the signal
- The cladding also consists of glass or plastic, but with a lower refractive index compared to the core
- The buffer protects the fiber from damage and moisture
- The jacket holds one or more fibers in a cable

Features:

- Lower cost
- Extremely wide bandwidth
- Lighter-weight and small
- More secure
- Resistant to corrosion
- Longer life and easy to maintain
- Elimination of cross-talk
- Immune to electrostatic interference

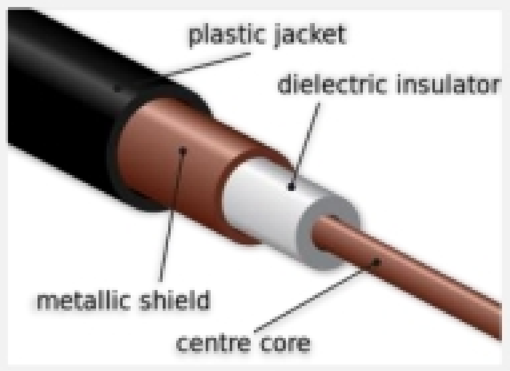


Types of Cables: Coaxial Cable

- Coaxial cable is a type of copper cable built with a metal shield and other components engineered to block signal interference
- It consists of two conductors separated by a dielectric material
- The center conductor and outer conductor are configured in such a way that they form a concentric cylinder with a common axis
- 50 ohm and 75 ohm coaxial cables are widely used
- A 50 ohm cable is used for digital transmission and a 75 ohm cable is used for analog transmission
- It has large bandwidth and low losses
- It has a data rate of 10 Mbps, which can be increased with an increase in the diameter of the inner conductor

Advantages:

- Cheap installation cost
- Great channel capacity
- Good bandwidth
- Easily modifiable
- Cheap production cost



Notes: ____

____

____

____

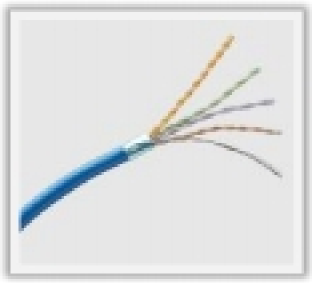
____

____

Types of Cables: CAT 3 and CAT 4

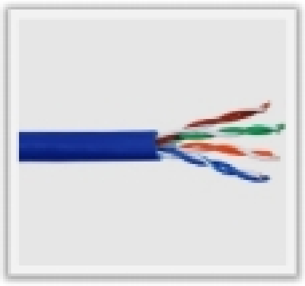
CAT 3

- Commonly known as Category 3 or station wire
- Used in voice application and 10 BaseT (10Mbps) Ethernet
- Bandwidth of 16 MHz
- Attenuation of 11.5 dB
- Impedance of 100 ohms



CAT 4

- Commonly known as Category 4 cable and consists of four unshielded twisted pair copper wires
- Used in 10 BaseT (10Mbps) Ethernet
- Bandwidth of 20 MHz
- Attenuation of 7.5 dB
- Impedance of 100 ohms



Types of Cables: CAT 5

CAT 5 (Category 5)

- It is an unshielded, twisted pair cable that is terminated with RJ 45 connectors
- It has a maximum length of 100 m and supports frequencies up to 100 MHz
- It is suitable for 10BASE-T, 100BASE-TX, and 1000BASE-T networking
- It carries telephonic and video signals
- Punch-down blocks and modular connectors are used to connect this cable

Features:

- It is applicable to most LAN topologies and is suitable for 4 and 16 Mbps UTP Token Ring Systems
- It has a 100 MHz bandwidth, 24.0 dB attenuation, and 100 Ohms impedance
- It is used for high speed data transmission

Notes: ____

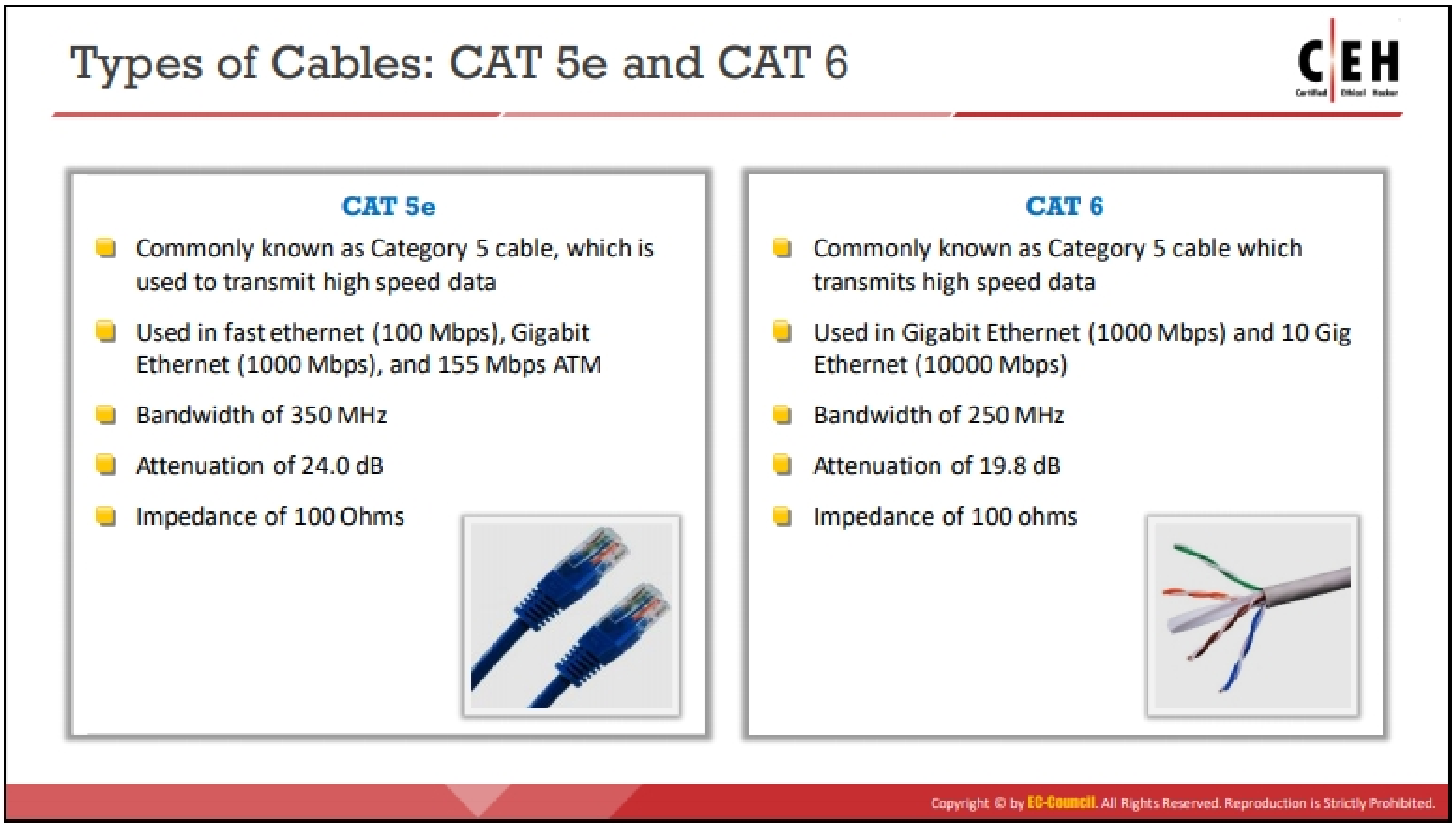
____

____

____

____

____



Types of Cables: CAT 5e and CAT 6

CAT 5e

- Commonly known as Category 5 cable, which is used to transmit high speed data
- Used in fast ethernet (100 Mbps), Gigabit Ethernet (1000 Mbps), and 155 Mbps ATM
- Bandwidth of 350 MHz
- Attenuation of 24.0 dB
- Impedance of 100 Ohms

CAT 6

- Commonly known as Category 5 cable which transmits high speed data
- Used in Gigabit Ethernet (1000 Mbps) and 10 Gig Ethernet (10000 Mbps)
- Bandwidth of 250 MHz
- Attenuation of 19.8 dB
- Impedance of 100 ohms

Types of Cables: 10/100/1000BaseT (UTP Ethernet)

- An ethernet connection method **uses twisted pair cables** and operates at 10, 100 or 1000 Mbps
- BASE denotes the **baseband transmission** and T stands for twisted pair cabling

10 Base-T

- Has a transmission speed of 10 Mbps and a maximum cable length of 100 m
- Uses 802.3i IEEE standard
- Cat 3 and Cat 5 are suitable
- Uses 4 wires (pins 1,2,3,6)

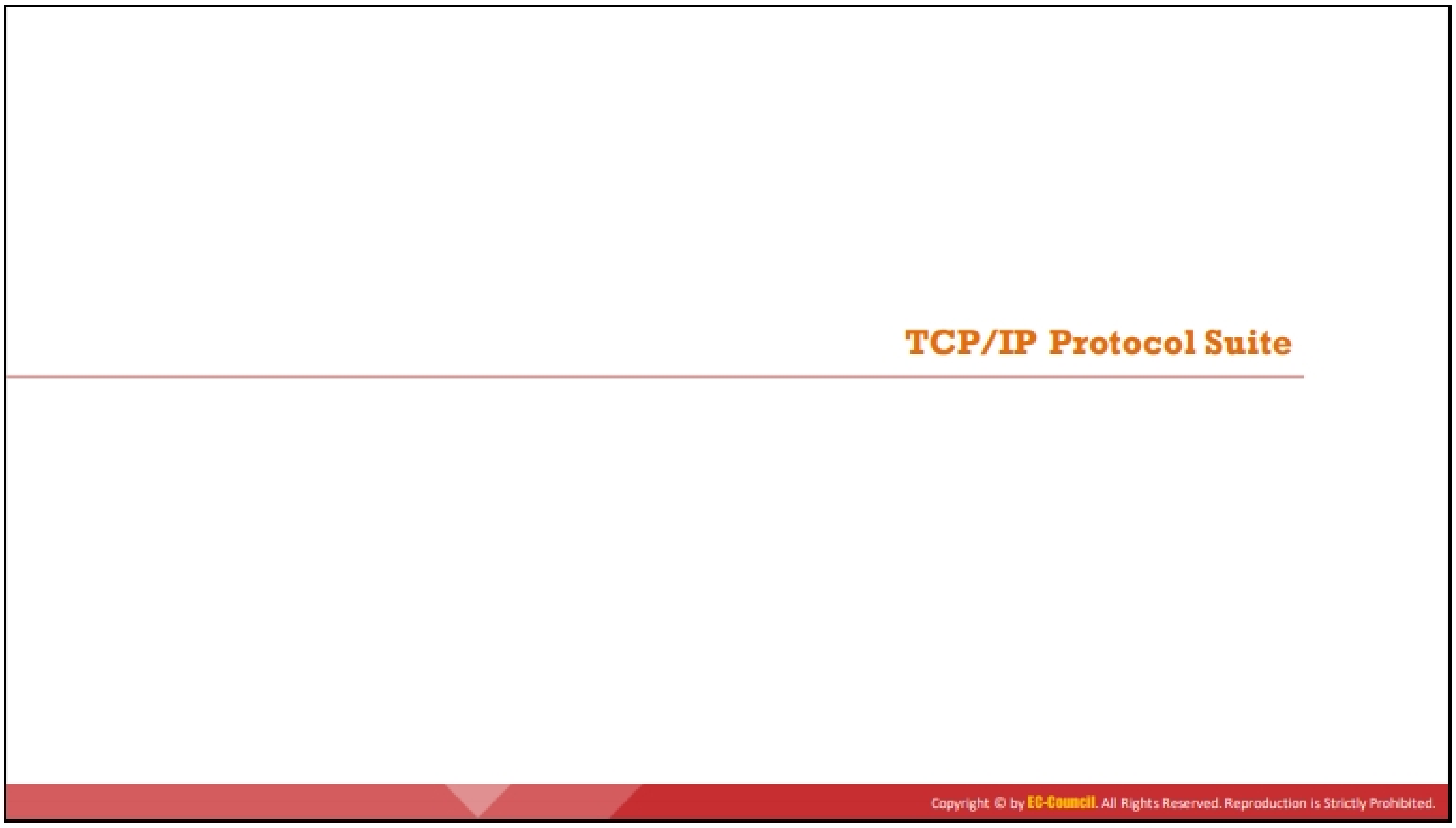
100 Base-T

- Has a transmission speed of 100 Mbps
- Uses 802.3u IEEE standard
- Cat 5 is suitable
- Uses 4 wires (pins 1,2,3,6)

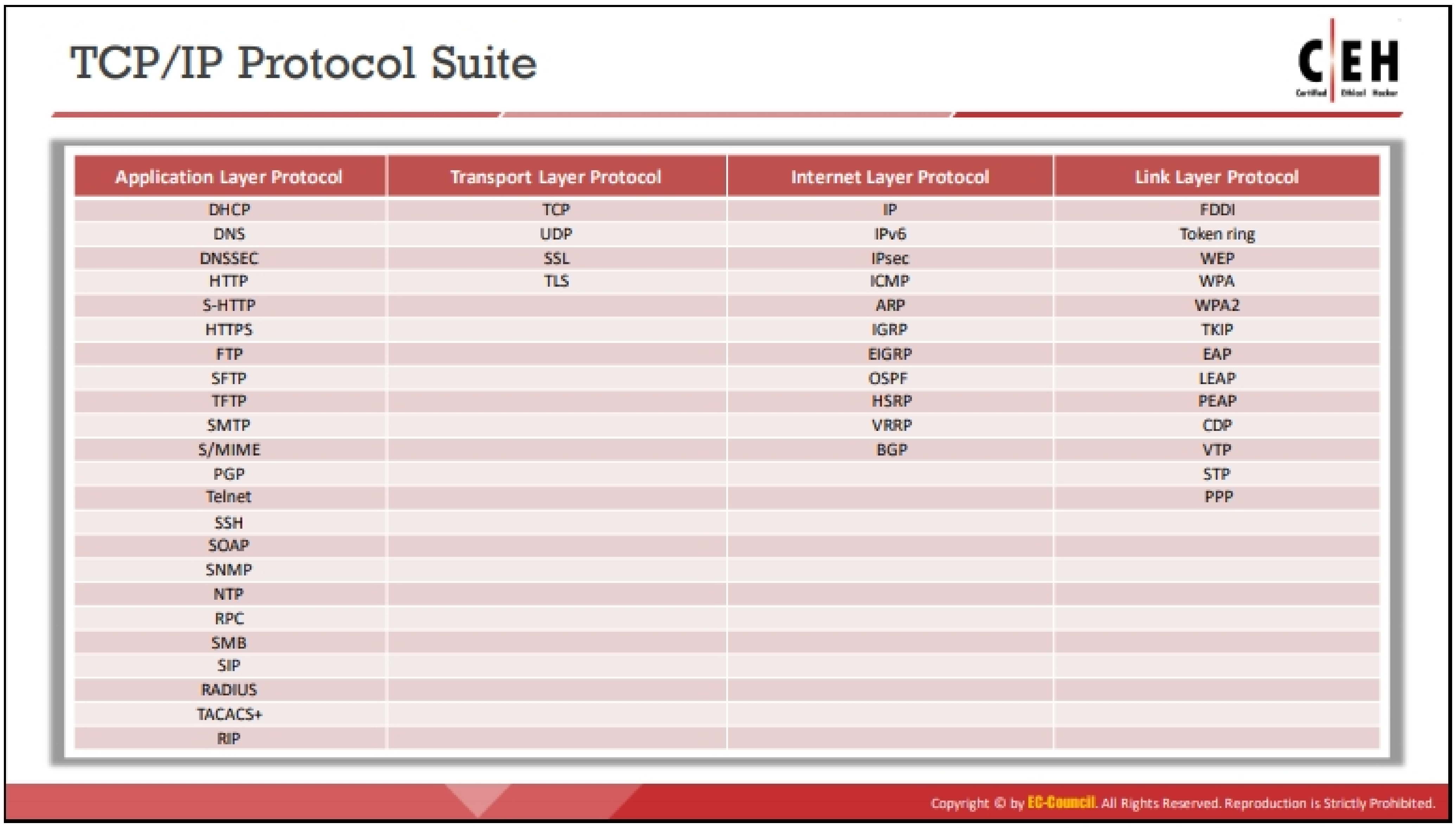
1000 Base-T

- Has a transmission speed of 1000 Mbps
- Uses 802.3ab IEEE standard
- Cat 5e is suitable cable
- Uses 8 wires (pins 1, 2, 3, 4, 5, 6, 7, 8)

Notes: ____



TCP/IP Protocol Suite



TCP/IP Protocol Suite

Application Layer Protocol	Transport Layer Protocol	Internet Layer Protocol	Link Layer Protocol
DHCP	TCP	IP	FDDI
DNS	UDP	IPv6	Token ring
DNSSEC	SSL	IPsec	WEP
HTTP	TLS	ICMP	WPA
S-HTTP		ARP	WPA2
HTTPS		IGRP	TKIP
FTP		EIGRP	EAP
SFTP		OSPF	LEAP
TFTP		HSRP	PEAP
SMTP		VRRP	CDP
S/MIME		BGP	VTP
PGP			STP
Telnet			PPP
SSH			
SOAP			
SNMP			
NTP			
RPC			
SMB			
SIP			
RADIUS			
TACACS+			
RIP			

Notes: ____

____

____

____

____

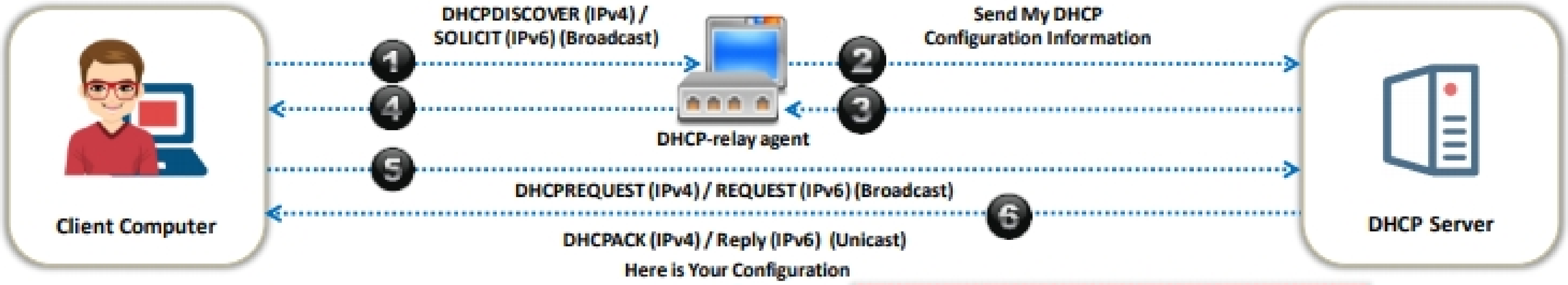
____

TCP/IP Protocol Suite

Application Layer Protocols

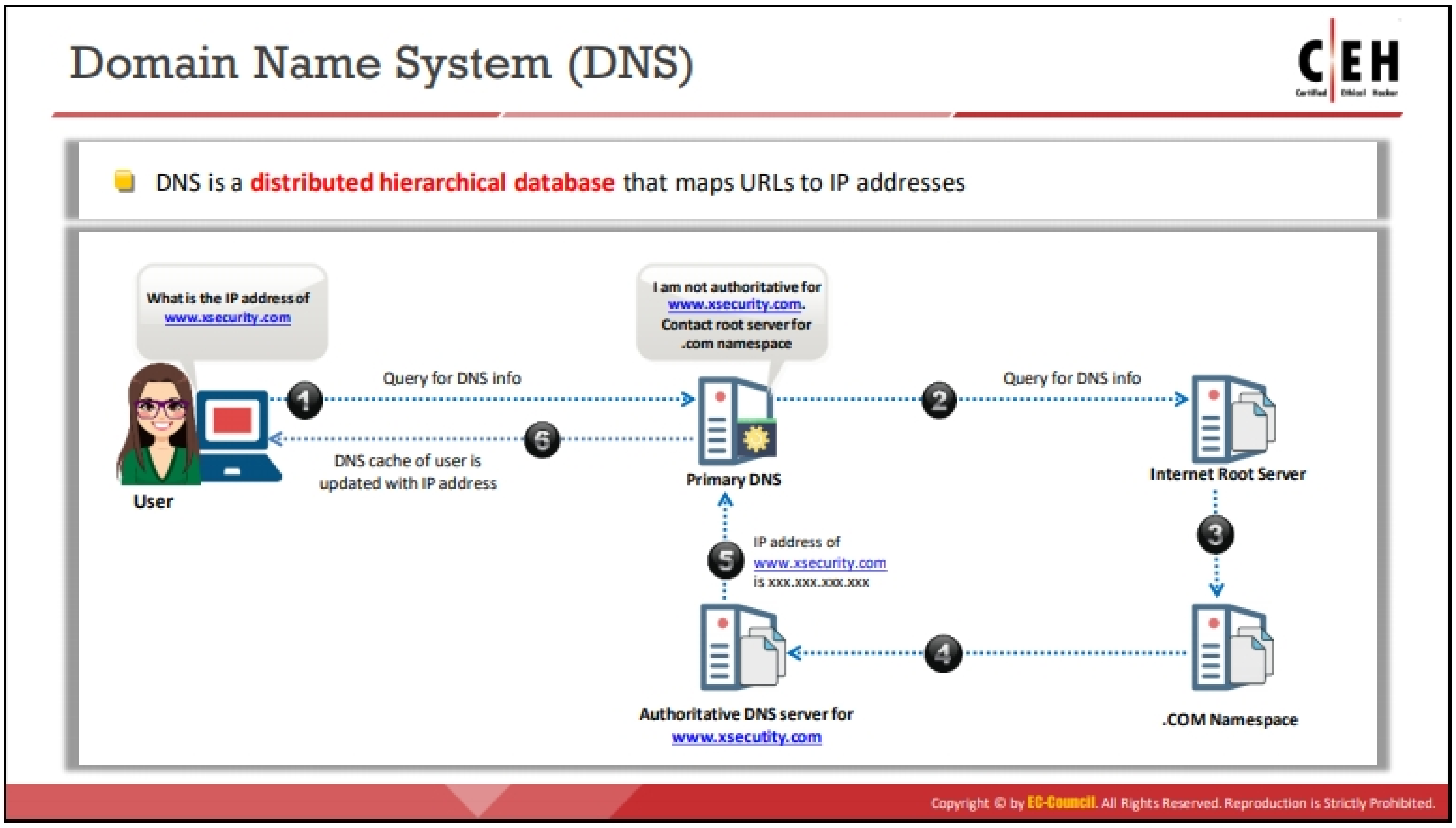
Dynamic Host Configuration Protocol (DHCP)

- DHCP is used by DHCP servers to **distribute TCP/IP configuration** information to DHCP-enabled clients in the form of a lease offer


DHCPDISCOVER (IPv4) / SOLICIT (IPv6) (Broadcast)
Send My DHCP Configuration Information
1
2
3
4
DHCP-relay agent
Client Computer
5
DHCPREQUEST (IPv4) / REQUEST (IPv6) (Broadcast)
6
DHCP Server
DHCPACK (IPv4) / Reply (IPv6) (Unicast)
Here is Your Configuration

```
IP Address: 10.0.0.20
Subnet Mask: 255.255.255.0
Default Routers: 10.0.0.1
DNS Servers: 192.168.168.2, 192.168.168.3
Lease Time: 2 days
```

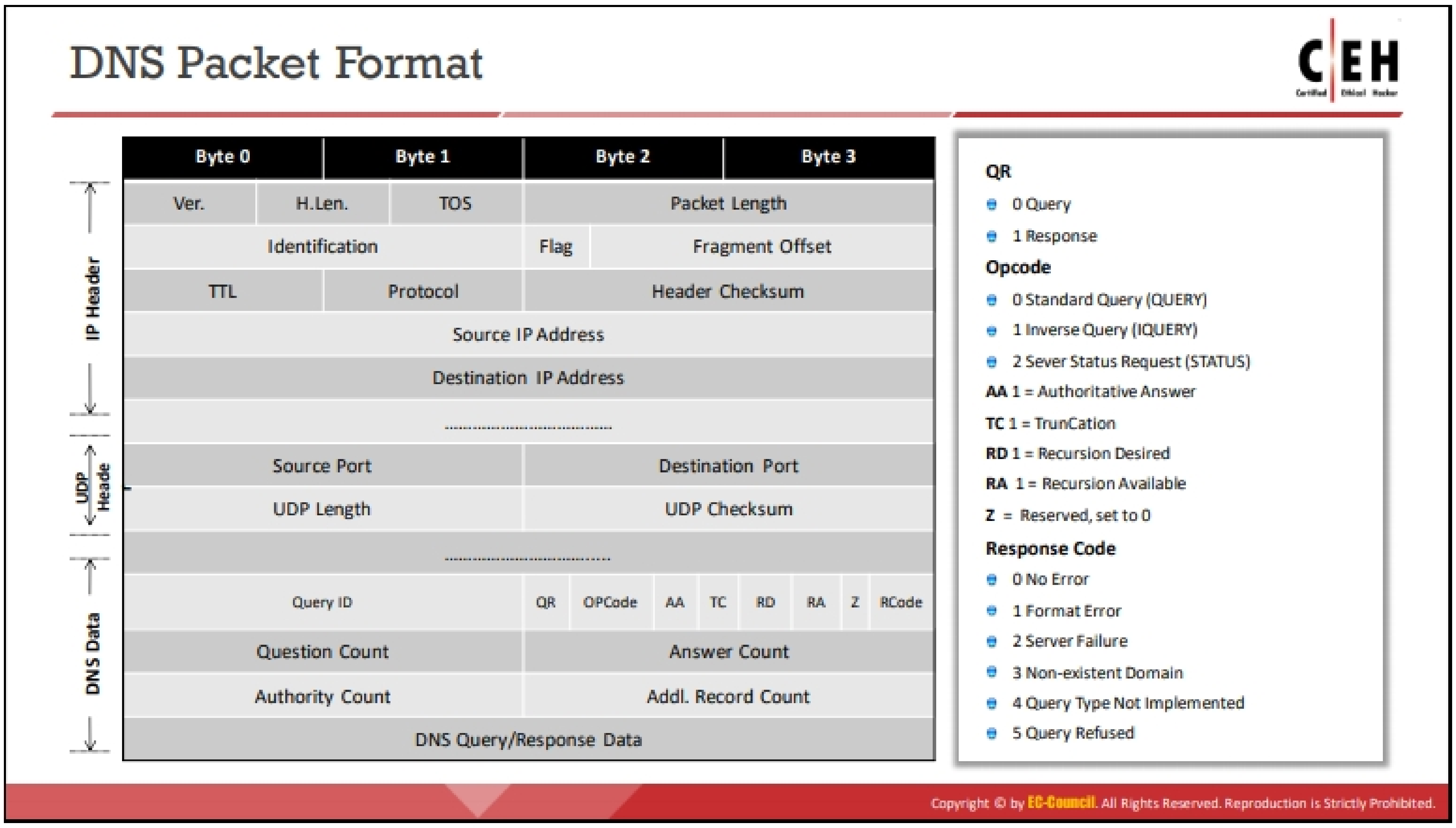
Notes: ____



Domain Name System (DNS)

- DNS is a **distributed hierarchical database** that maps URLs to IP addresses

What is the IP address of www.xsecurity.com
User
1
Query for DNS info
6
DNS cache of user is updated with IP address
I am not authoritative for www.xsecurity.com. Contact root server for .com namespace
Primary DNS
2
Query for DNS info
Internet Root Server
3
.COM Namespace
4
Authoritative DNS server for www.xsecutity.com
5
IP address of www.xsecurity.com is xxx.xxx.xxx.xxx



DNS Packet Format

<table>
<tr><th></th><th colspan="6">Byte 0</th><th colspan="6">Byte 1</th><th colspan="6">Byte 2</th><th colspan="6">Byte 3</th></tr>
<tr><td rowspan="5">IP Header</td><td colspan="4">Ver.</td><td colspan="4">H.Len.</td><td colspan="4">TOS</td><td colspan="12">Packet Length</td></tr>
<tr><td colspan="12">Identification</td><td colspan="2">Flag</td><td colspan="10">Fragment Offset</td></tr>
<tr><td colspan="6">TTL</td><td colspan="6">Protocol</td><td colspan="12">Header Checksum</td></tr>
<tr><td colspan="24">Source IP Address</td></tr>
<tr><td colspan="24">Destination IP Address</td></tr>
<tr><td></td><td colspan="24">……………………………</td></tr>
<tr><td rowspan="2">UDP Heade</td><td colspan="12">Source Port</td><td colspan="12">Destination Port</td></tr>
<tr><td colspan="12">UDP Length</td><td colspan="12">UDP Checksum</td></tr>
<tr><td></td><td colspan="24">……………………………</td></tr>
<tr><td rowspan="4">DNS Data</td><td colspan="12">Query ID</td><td>QR</td><td colspan="2">OPCode</td><td>AA</td><td>TC</td><td colspan="2">RD</td><td colspan="2">RA</td><td>Z</td><td colspan="2">RCode</td></tr>
<tr><td colspan="12">Question Count</td><td colspan="12">Answer Count</td></tr>
<tr><td colspan="12">Authority Count</td><td colspan="12">Addl. Record Count</td></tr>
<tr><td colspan="24">DNS Query/Response Data</td></tr>
</table>

QR

- 0 Query
- 1 Response

Opcode

- 0 Standard Query (QUERY)
- 1 Inverse Query (IQUERY)
- 2 Sever Status Request (STATUS)

AA 1 = Authoritative Answer

TC 1 = TrunCation

RD 1 = Recursion Desired

RA 1 = Recursion Available

Z = Reserved, set to 0

Response Code

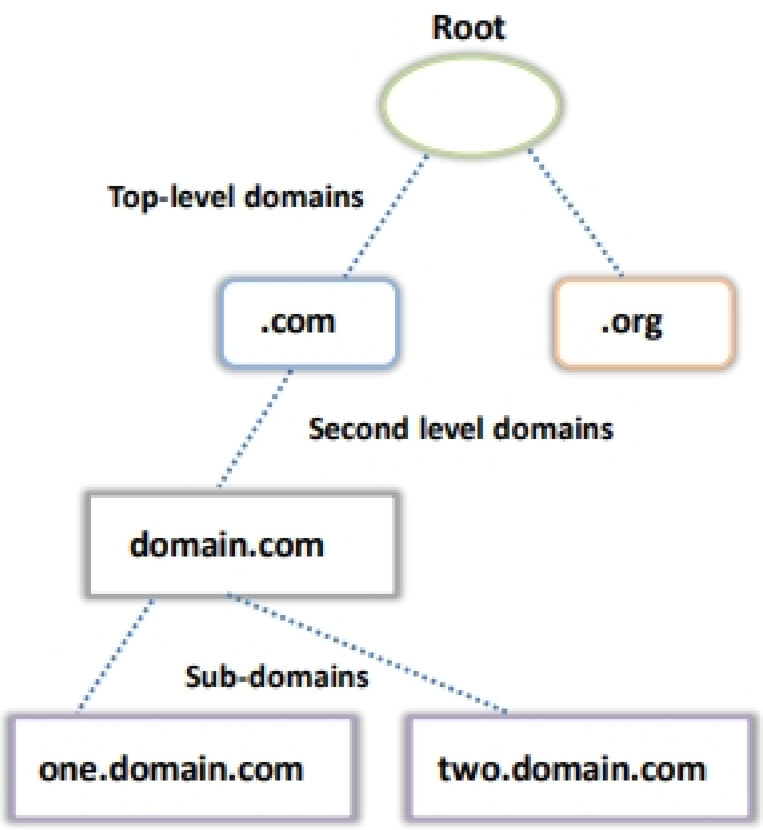
- 0 No Error
- 1 Format Error
- 2 Server Failure
- 3 Non-existent Domain
- 4 Query Type Not Implemented
- 5 Query Refused

Notes: ______________________________

DNS Hierarchy

The DNS hierarchy comprises:

- **Root level domain**: The highest domain of all the domains in the hierarchy, it responds to requests and contains information about the global list of top-level domains such as .com, .org, .uk, or .nz
- **Top level domains**: Contains two types of domains, such as organizational and geographical hierarchies
- **Second level domains**: The actual domain name that varies from owner to owner. It can be named as per the user's desire and without any restrictions
- **Sub-domains**: When the main domain is split into parts, these parts are called sub-domains. For example, if an organization has its main domain as mydomain.com, then about.mydomain.com and contact.mydomain.com could be its sub-domains
- **Host**: The device that contains the DNS hierarchy domain names



DNSSEC

- Domain Name System Security Extensions (DNSSEC) is a suite of the Internet Engineering Task Force (IETF)
- It is used for securing certain types of information provided by DNS
- It works by digitally signing records for DNS lookup using public-key cryptography

DNSSEC guarantees:

- Authenticity
- Integrity
- The non-existence of a domain name or type

DNSSEC does not guarantee:

- Confidentiality
- Protection against Denial of Service (DoS)

Notes: ____

How DNSSEC Works

1. DNSSEC is based on the concept of **asymmetric keys** — Public and private keys
2. DNSSEC adds a **digital signature** to each piece of a domain name's DNS information
3. When a guest enters the domain name's URL in a web browser, the **resolver verifies** the digital signature
4. The digital signature must match the **value on file at the registry**; else, the resolver will reject the response

Managing DNSSEC for Domain Name

1. DNSSEC adds a layer of security to domain names by adding **digital signatures** to the **Domain Name System** (DNS) information
2. **Delegation Signing** (DS) data contain the digital signature information for a respective domain name's DNS
3. The following are the extensions that can be managed in DS records:
   - .com; .net; .biz; .us; .org; .eu; .co.uk, .me.uk, and .org.uk; .co; .com.co, .net.co, and .nom.co
4. Depending upon the domain name's extension, one or more **DS records can be used at a time**

Notes: ____

What is a DS Record?

- Delegation Signing (DS) records provide complete information about a **signed zone file**
- Allowing DNSSEC for domain name requires this information to complete the setup of a **signed domain name**

How does DNSSEC Protect Internet Users?

- DNSSEC is built to shield Internet users from **artificial DNS data**, such as a deceptive or mischievous address instead of a genuine address that was requested
- There are differences between non-aware and DNSSEC-aware lookups:

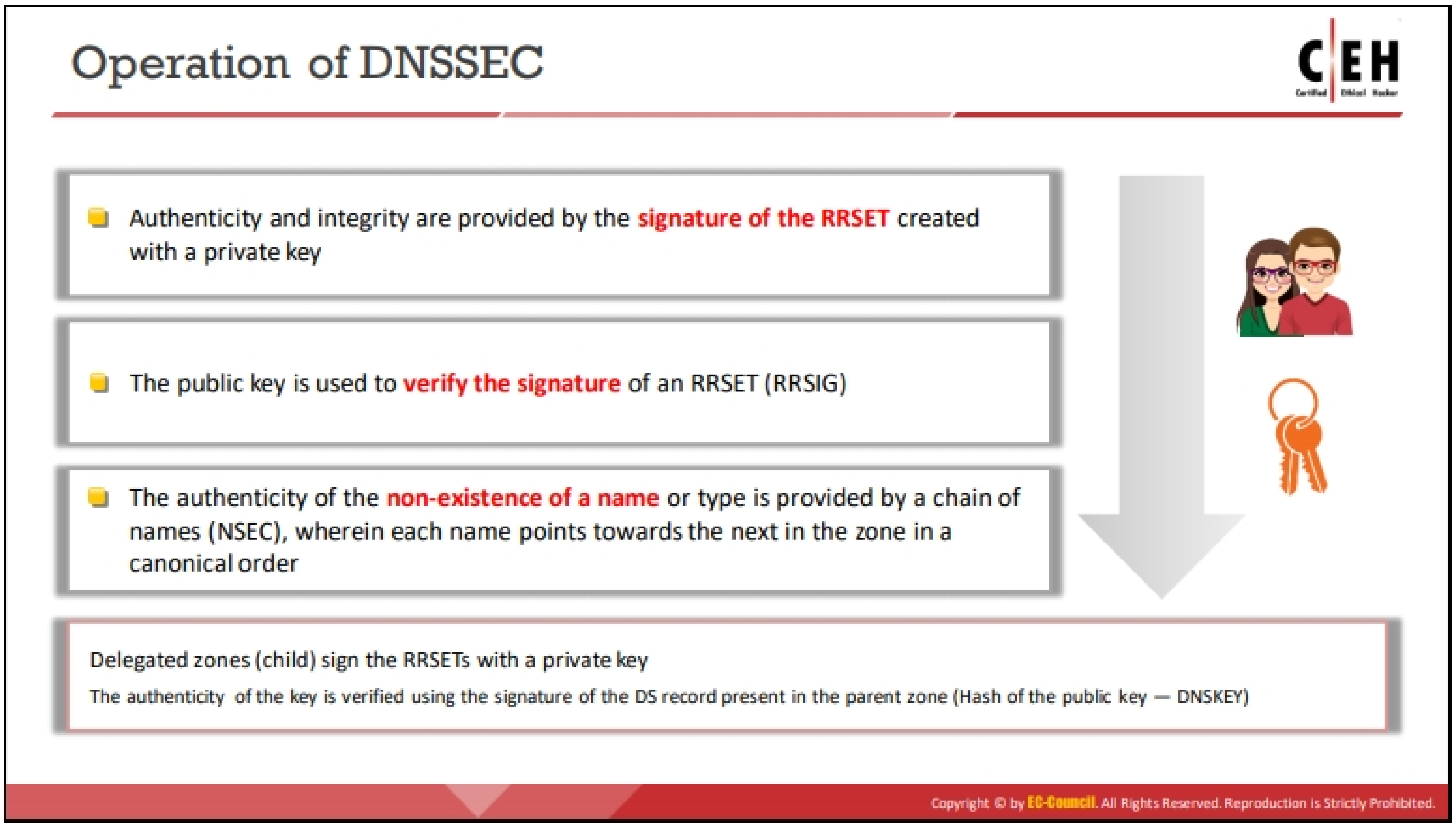
Non-DNSSEC-Aware Lookups

- The URL request goes onto the Internet and accepts the first response it receives
- A mischievous Internet user can cut off the request and send back incorrect information
- The response received points to an undesired Internet site where personal data can be compromised

DNSSEC-Aware Lookups

- These DNS lookups travel toward the domain name's registry and receive a duplicate of the digital signature that is being used by the URL
- The browser cannot display the site unless an address response also includes the matching digital signature
- This forestalls misdirection to a bogus location instead of the one requested

Notes:

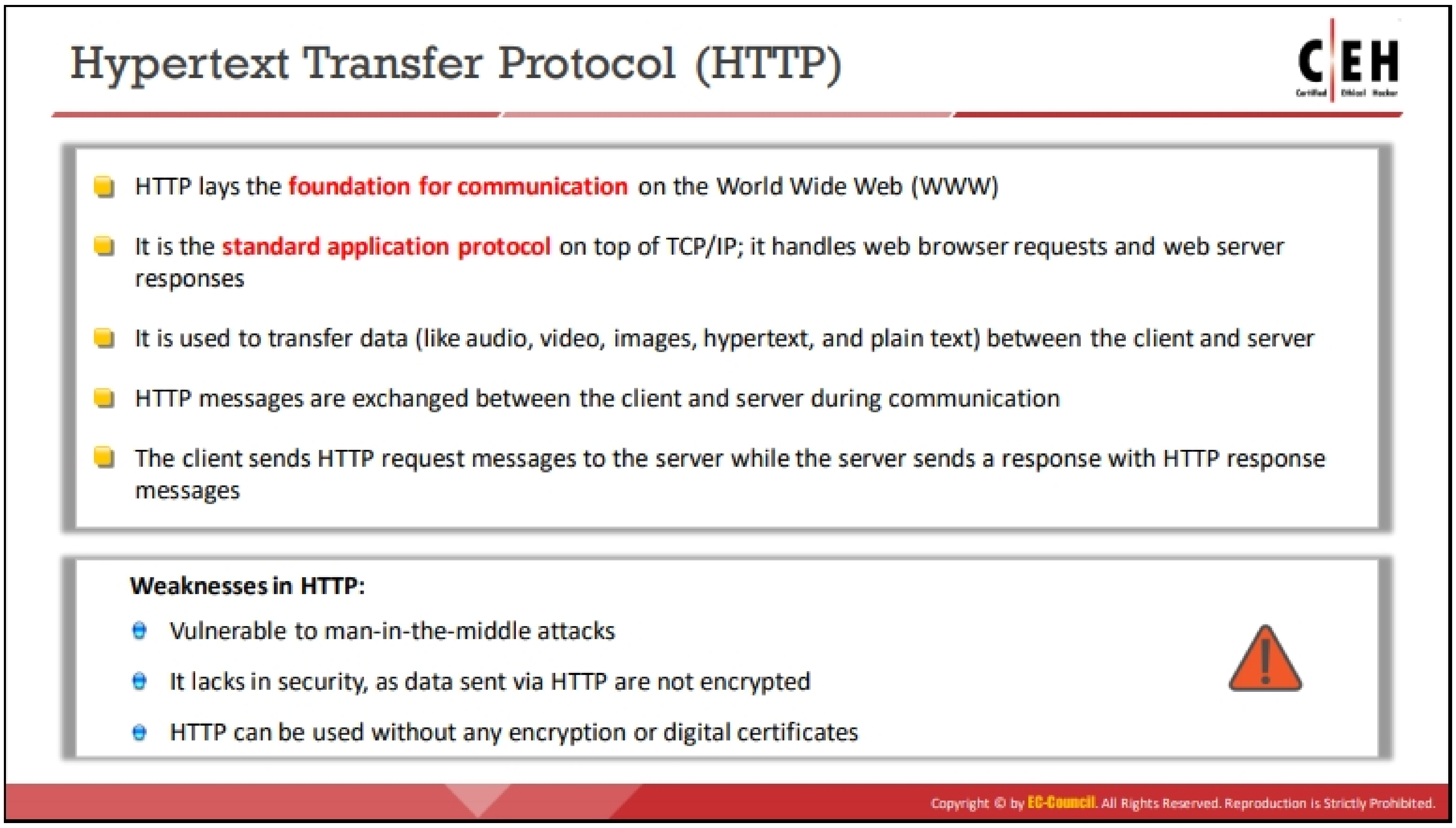


Operation of DNSSEC

- Authenticity and integrity are provided by the **signature of the RRSET** created with a private key
- The public key is used to **verify the signature** of an RRSET (RRSIG)
- The authenticity of the **non-existence of a name** or type is provided by a chain of names (NSEC), wherein each name points towards the next in the zone in a canonical order

Delegated zones (child) sign the RRSETs with a private key

The authenticity of the key is verified using the signature of the DS record present in the parent zone (Hash of the public key — DNSKEY)



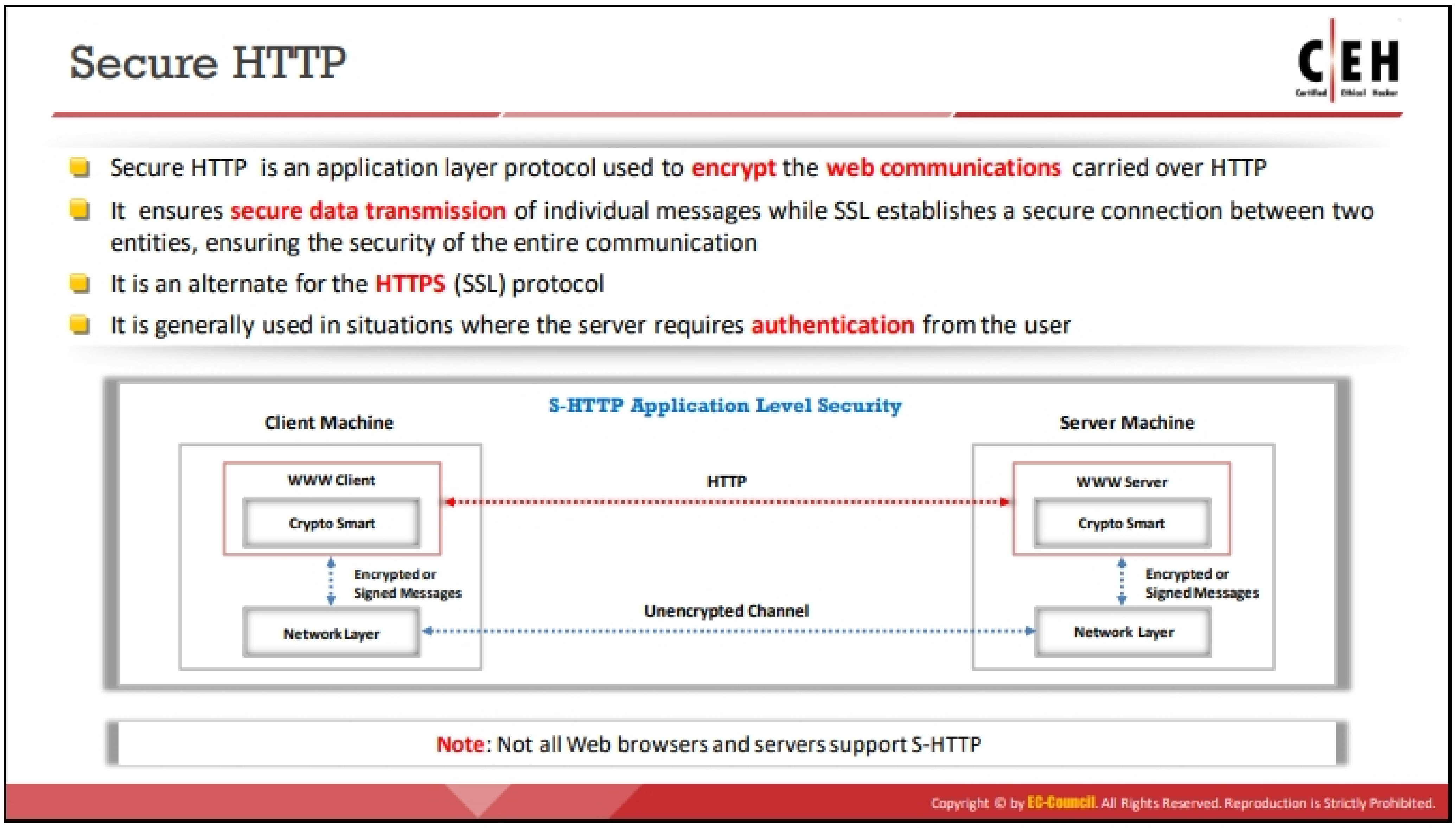
Hypertext Transfer Protocol (HTTP)

- HTTP lays the **foundation for communication** on the World Wide Web (WWW)
- It is the **standard application protocol** on top of TCP/IP; it handles web browser requests and web server responses
- It is used to transfer data (like audio, video, images, hypertext, and plain text) between the client and server
- HTTP messages are exchanged between the client and server during communication
- The client sends HTTP request messages to the server while the server sends a response with HTTP response messages

Weaknesses in HTTP:

- Vulnerable to man-in-the-middle attacks
- It lacks in security, as data sent via HTTP are not encrypted
- HTTP can be used without any encryption or digital certificates

Notes: ____



Secure HTTP

- Secure HTTP is an application layer protocol used to **encrypt** the **web communications** carried over HTTP
- It ensures **secure data transmission** of individual messages while SSL establishes a secure connection between two entities, ensuring the security of the entire communication
- It is an alternate for the **HTTPS** (SSL) protocol
- It is generally used in situations where the server requires **authentication** from the user

S-HTTP Application Level Security

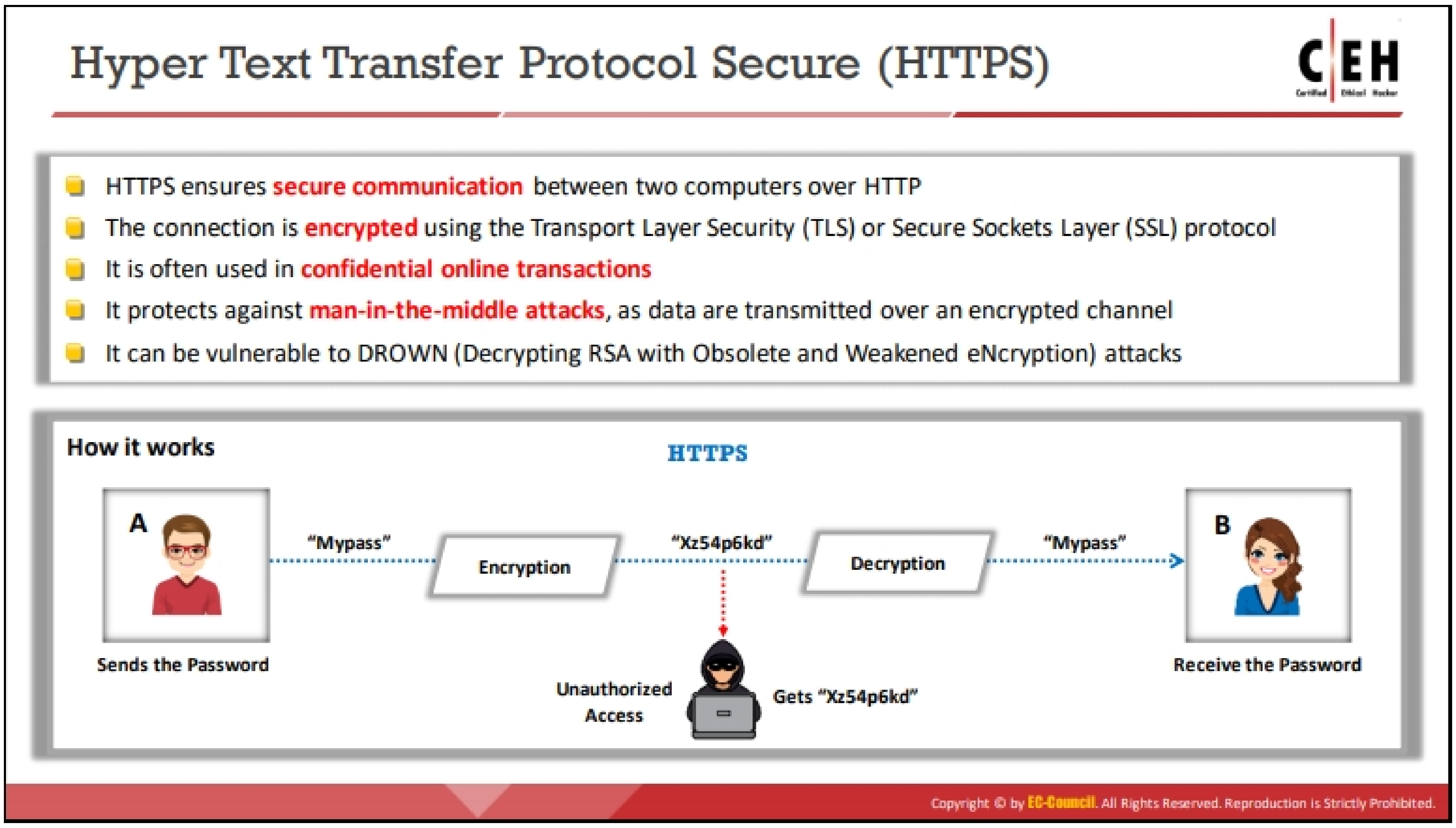
Client Machine
WWW Client
Crypto Smart
Encrypted or Signed Messages
Network Layer

HTTP

Unencrypted Channel

Server Machine
WWW Server
Crypto Smart
Encrypted or Signed Messages
Network Layer

Note: Not all Web browsers and servers support S-HTTP



Hyper Text Transfer Protocol Secure (HTTPS)

- HTTPS ensures **secure communication** between two computers over HTTP
- The connection is **encrypted** using the Transport Layer Security (TLS) or Secure Sockets Layer (SSL) protocol
- It is often used in **confidential online transactions**
- It protects against **man-in-the-middle attacks**, as data are transmitted over an encrypted channel
- It can be vulnerable to DROWN (Decrypting RSA with Obsolete and Weakened eNcryption) attacks

How it works

HTTPS

A
Sends the Password
"Mypass"
Encryption
"Xz54p6kd"
Decryption
"Mypass"
B
Receive the Password
Unauthorized Access
Gets "Xz54p6kd"

Notes:

File Transfer Protocol (FTP)

- File Transfer Protocol (FTP) is a standard networking **protocol used for sharing files** over the Internet's TCP/IP protocols
- Based on the **client-server architecture**, FTP uses SSL/TLS and SSH encryptions for data security
- FTP servers provide access to users using a simple login mechanism

How FTP Works?

FTP uses two connections:

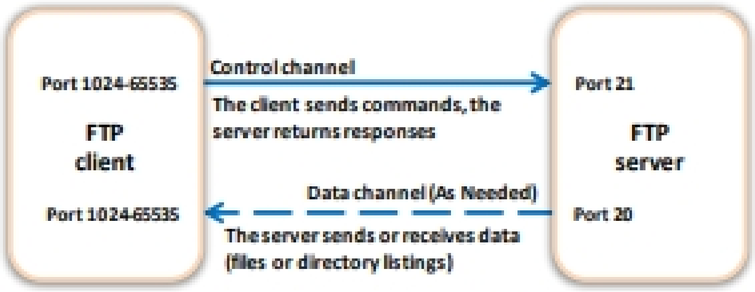
- **Control connection** — transmits commands and the replies to those commands between the client and the server
- **Data connection** — for the transfer of data files

FTP supports two modes of operation

Active Mode

- The control connection is made from the FTP client, and all data connections are made from the FTP server to the FTP client

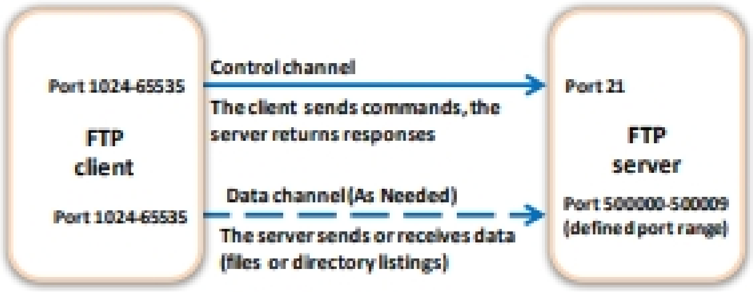
Active FTP: control In, Data Out


Port 1024-65535
FTP client
Port 1024-65535
Control channel
The client sends commands, the server returns responses
Data channel (As Needed)
The server sends or receives data (files or directory listings)
Port 21
FTP server
Port 20

Passive Mode

- Both the control and data connections are established from the FTP client to the FTP server

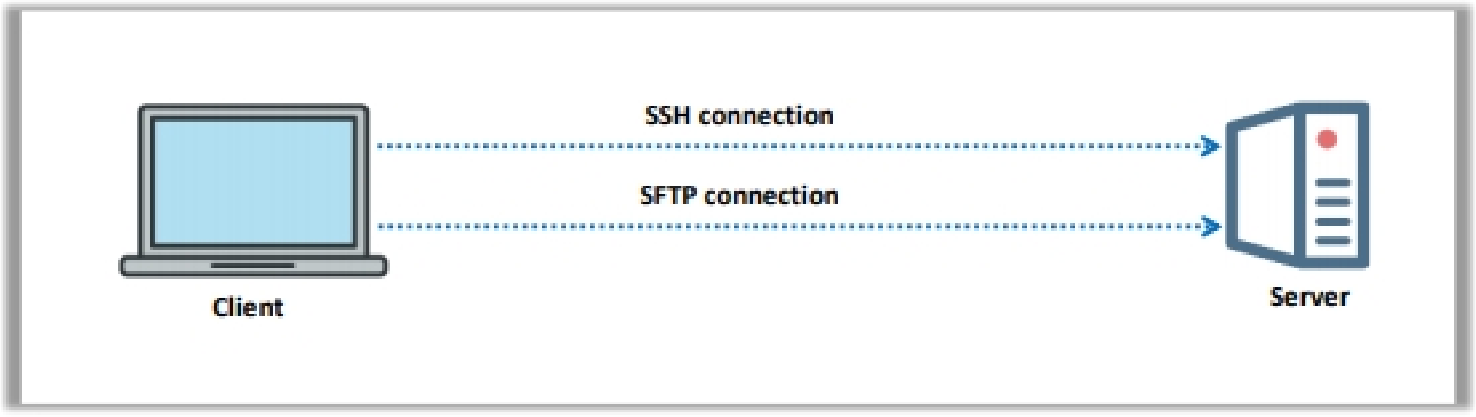
Passive FTP: Both connections Inbound


Port 1024-65535
FTP client
Port 1024-65535
Control channel
The client sends commands, the server returns responses
Data channel (As Needed)
The server sends or receives data (files or directory listings)
Port 21
FTP server
Port 500000-500009 (defined port range)

Notes: ____

Secure File Transfer Protocol (SFTP)

- SFTP is a **secure version of FTP** and an extension of SSH2 protocol
- It is used for secure file transmission and file access over a reliable data stream
- It runs on **TCP port 22**



Trivial File Transfer Protocol (TFTP)

- TFTP is a **lockstep communication protocol**
- It transmits files in both directions of a client-server application
- It help in node booting on a local area network when the operating system or firmware images are stored on a file server
- TFTP only reads and writes files from or to a remote server. It cannot list, delete, or rename files or directories, and it has no provisions for user authentication
- TFTP is generally used only with **local area networks (LAN)**
- TFTP constitutes an **independent exchange**

Weaknesses:

- It is vulnerable to denial of service (DoS) attacks
- It is vulnerable to directory traversal vulnerability

Notes: ____

____

____

____

____

____

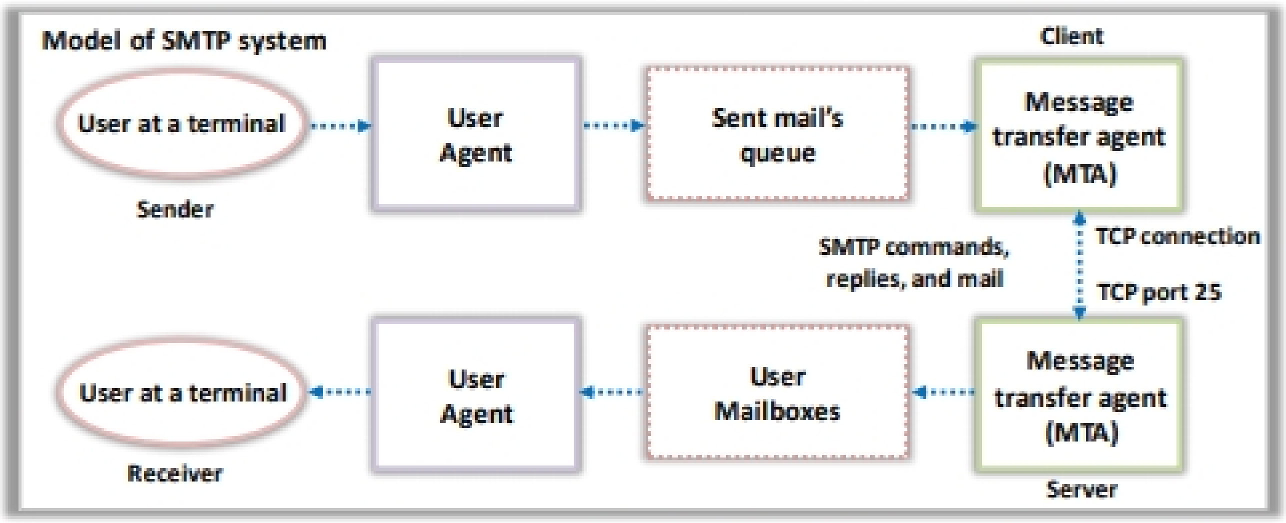
Simple Mail Transfer Protocol (SMTP)

- SMTP is an application layer protocol for **electronic mail (email) transmission**
- It is a relatively **simple and text-based protocol** that communicates with the mail server over TCP port 25
- There are two types of SMTP model
  - End to end: Used to communicate between different organizations
  - Store and forward : Used to communicate within an organization

Features:

- Mail forwarding
- Mail gatewaying
- Mail relaying
- Address debugging
- Mailing list expansion

Model of SMTP system


Client
User at a terminal
Sender
User Agent
Sent mail's queue
Message transfer agent (MTA)
SMTP commands, replies, and mail
TCP connection
TCP port 25
User at a terminal
Receiver
User Agent
User Mailboxes
Message transfer agent (MTA)
Server

Simple Mail Transfer Protocol (SMTP) (Cont'd)

Advantages:

- SMTP provides the simplest form of communication through mail
- Quick email delivery
- It is reliable for outgoing email messages
- Easy to connect and can be connected to any system that is flexible with existing applications
- Can be used on several platforms
- Incurs low implementation and administration cost

Disadvantages:

- Security is weakest for SMTP
- Limited to 7 bit ASCII characters
- Lacks the security protocols specified in X.400
- Usefulness is limited owing to its simplicity

Notes: ____

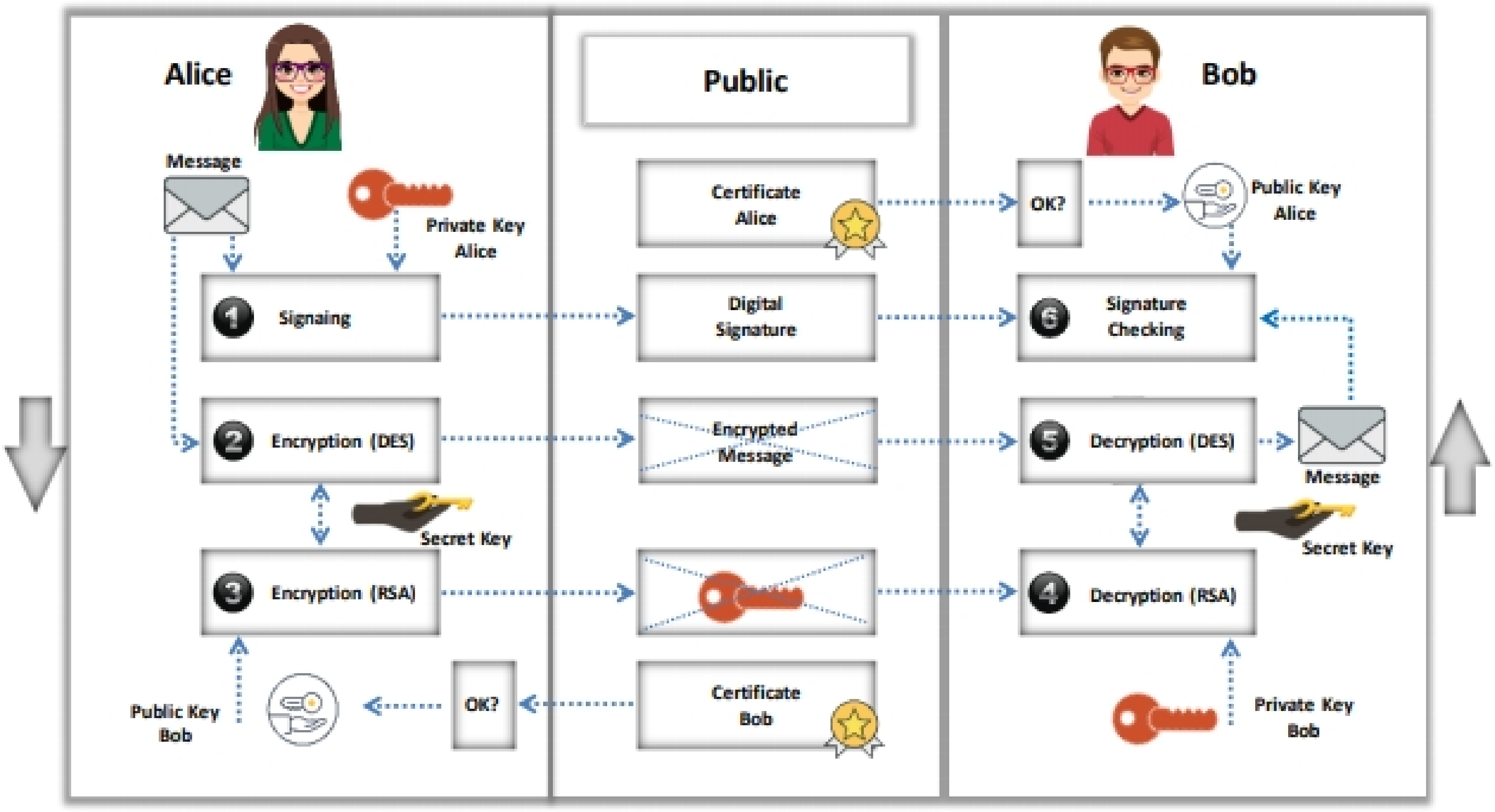
S/MIME

1 S/MIME (Secure/Multipurpose Internet Mail Extensions) is an application layer protocol which is used to send **digitally signed** and **encrypted email messages**

2 It uses **RSA** for its digital signature and DES for message encryption

3 Administrators need to **enable** S/MIME-based security for the mailboxes in their organizations

How it Works?

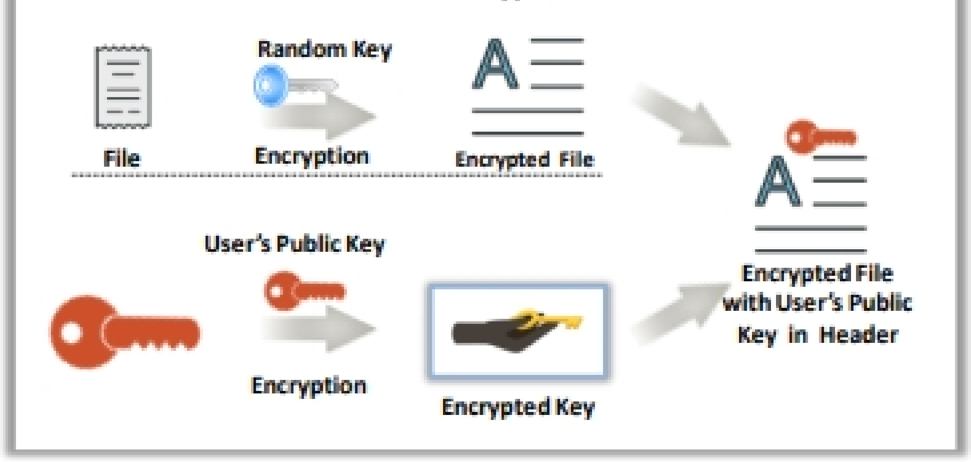

Alice
Public
Bob
Message
Private Key Alice
Certificate Alice
OK?
Public Key Alice
1 Signaing
Digital Signature
6 Signature Checking
2 Encryption (DES)
Encrypted Message
5 Decryption (DES)
Message
Secret Key
3 Encryption (RSA)
4 Decryption (RSA)
Secret Key
Public Key Bob
OK?
Certificate Bob
Private Key Bob

Notes: ____

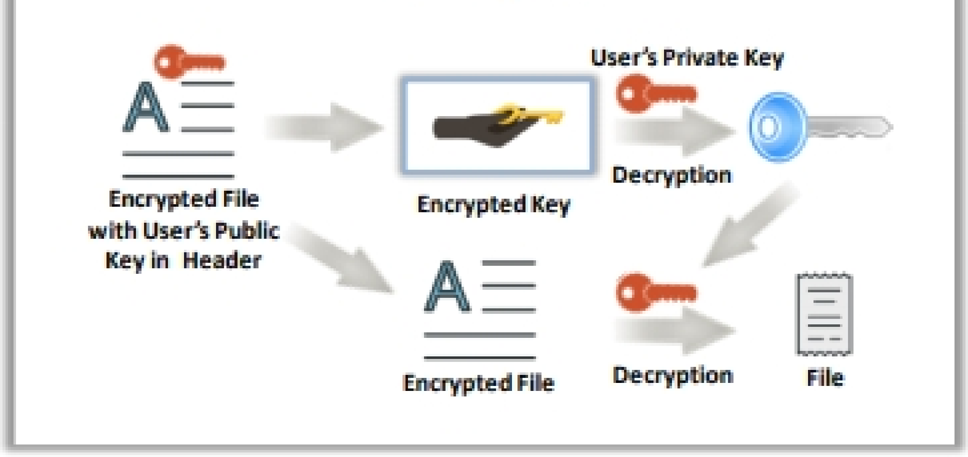
Pretty Good Privacy (PGP)

- PGP is an application layer protocol that provides **cryptographic privacy** and authentication for network communication
- It encrypts and decrypts email communication and authenticates messages with **digital signatures** and encrypts stored files

File Encryption


File
Random Key
Encryption
Encrypted File
User's Public Key
Encryption
Encrypted Key
Encrypted File with User's Public Key in Header

File Decryption


Encrypted File with User's Public Key in Header
Encrypted Key
User's Private Key
Decryption
Encrypted File
Decryption
File

Difference between PGP and S/MIME

Mandatory Features	S/MIME v3	OpenPGP
Message Format	Binary, Based on CMS	Application/Pkcs 7-mime
Certificate Format	Binary, Based on X.509v3	Binary, Based on previous PGP
Symmetric Encryption Algorithm	Triple DES (DES, EDE3, and CBC)	Triple DES (DES, EDE3, and Eccentric CFB)
Signature Algorithm	Diffie-Hellman (X9.42) with DSS or RSA	ElGamal with DSS
Hash Algorithm	SHA- 1	SHA- 1
MIME Encapsulation of Signed Data	Choice of Multipart/signed or CMS Format	Multipart/signed ASCII armor
MIME Encapsulation of Encrypted Data	Application/Pkcs 7-mime	Multipart/Encrypted

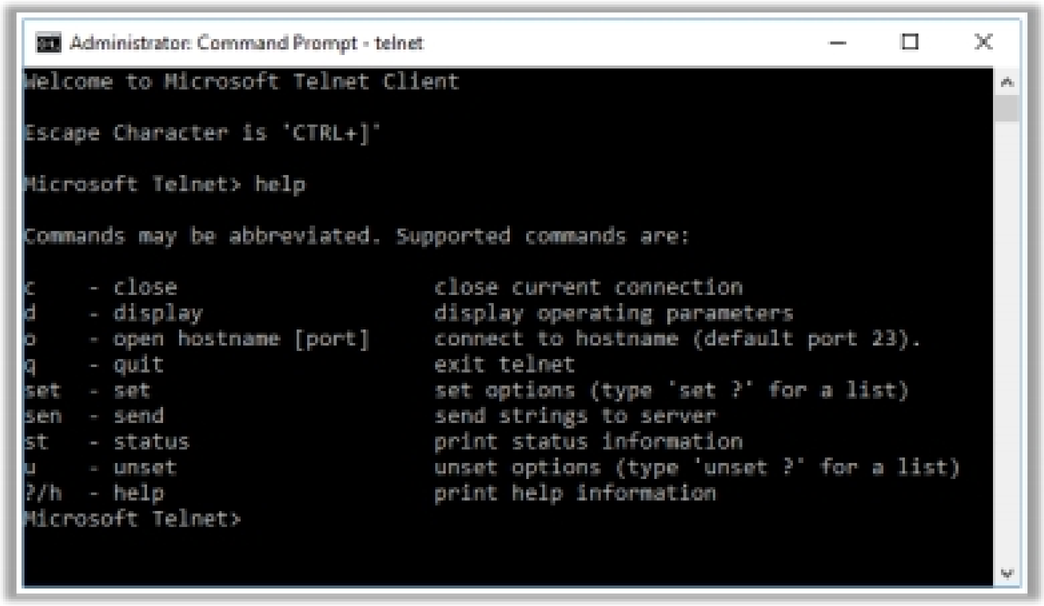
Notes: ______________________________

Telnet

- Telnet (telecommunications network) is a **TCP/IP protocol** used on a LAN that helps a user or administrator to **access** remote computers over a network

Advantages

- Allows logging on to a remote computer and executing programs
- Allows controlling Web servers remotely and enabling communication with other servers on the network
- Fast and efficient even when the network and system loads are high



```
Welcome to Microsoft Telnet Client

Escape Character is 'CTRL+]'

Microsoft Telnet> help

Commands may be abbreviated. Supported commands are:

c    - close                    close current connection
d    - display                  display operating parameters
o    - open hostname [port]     connect to hostname (default port 23).
q    - quit                     exit telnet
set  - set                      set options (type 'set ?' for a list)
sen  - send                     send strings to server
st   - status                   print status information
u    - unset                    unset options (type 'unset ?' for a list)
?/h  - help                     print help information
Microsoft Telnet>
```

Weaknesses

- Vulnerable to denial of service attacks
- Vulnerable to Packet sniffing attacks
- Telnet is not secure; it passes all data in clear text
- Eavesdropping attacks are also possible on the telnet network

SSH

- SSH, also known as **Secure Shell**, is another network management protocol. It is primarily used in UNIX and Linux environments
- It is mainly used for **secure remote login**
- It builds a secure, **encrypted tunnel** for exchanging information between the network management software and the devices
- Here, administrators must provide a username, password, and port number combination for authentication

SSH Authentication Mechanism

1. **Simple Authentication:** Authentication is performed based on the user's password
2. **Key-based Authentication:** SSH allows key-based authentication
    - The user needs to generate a public and a private key
    - These keys are generated using ssh-keygen -t rsa or ssh-keygen -t dsa
    - The private keys are used by the users the next time they try to establish a connection
    - The public key must be saved in ~/.ssh/authorized_keys
3. **Host-based authentication:** If the host-based authentication is enabled on the target machine, then users on a trusted host can log on to the target machine using the same username. To enable this feature, set setuid bit on /usr/lib/ssh/ssh-keysign (32-bit systems) or/usr/lib64/ssh/ssh-keysign (64-bit systems)

Notes: ____

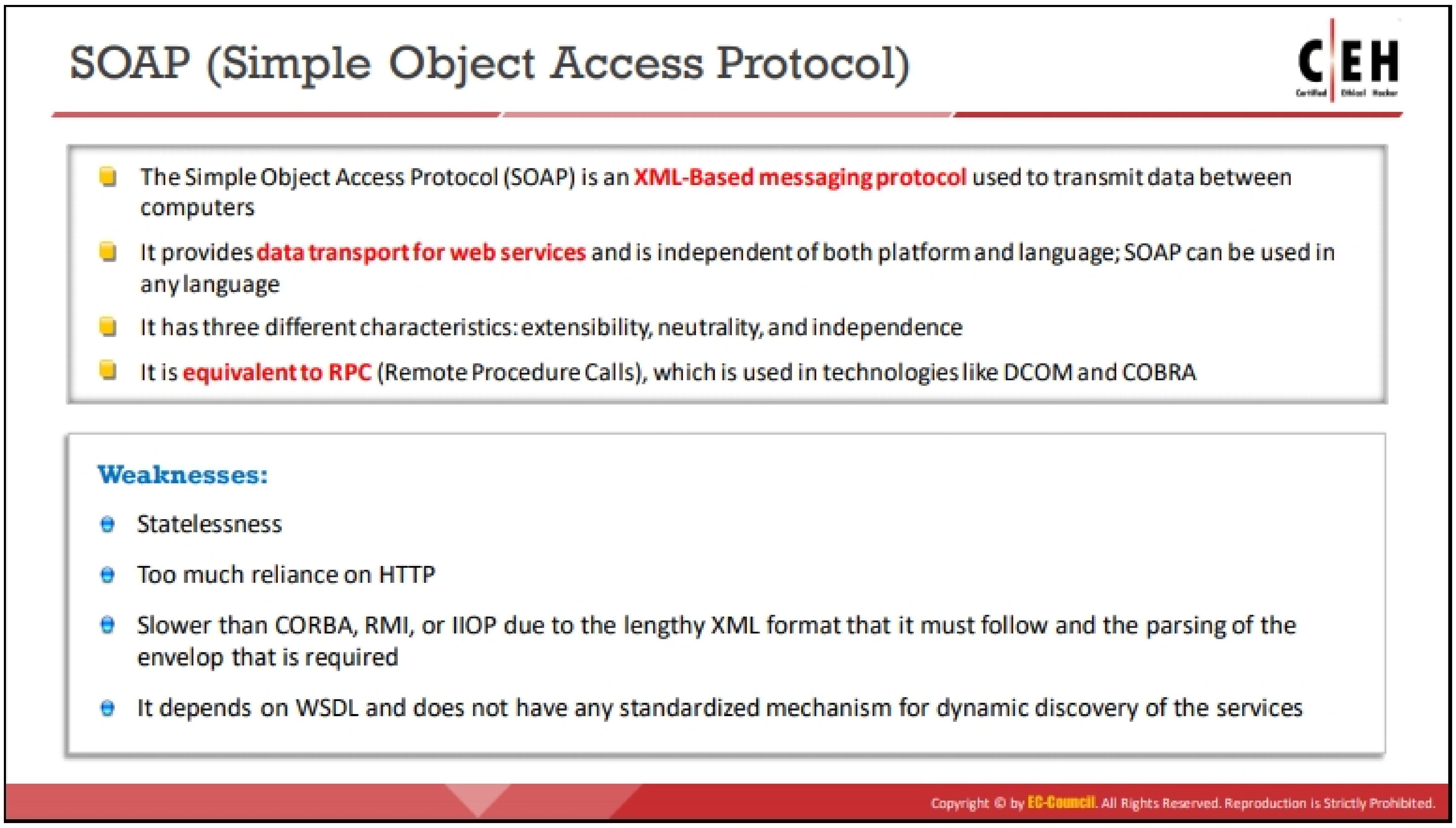
____

____

____

____

____

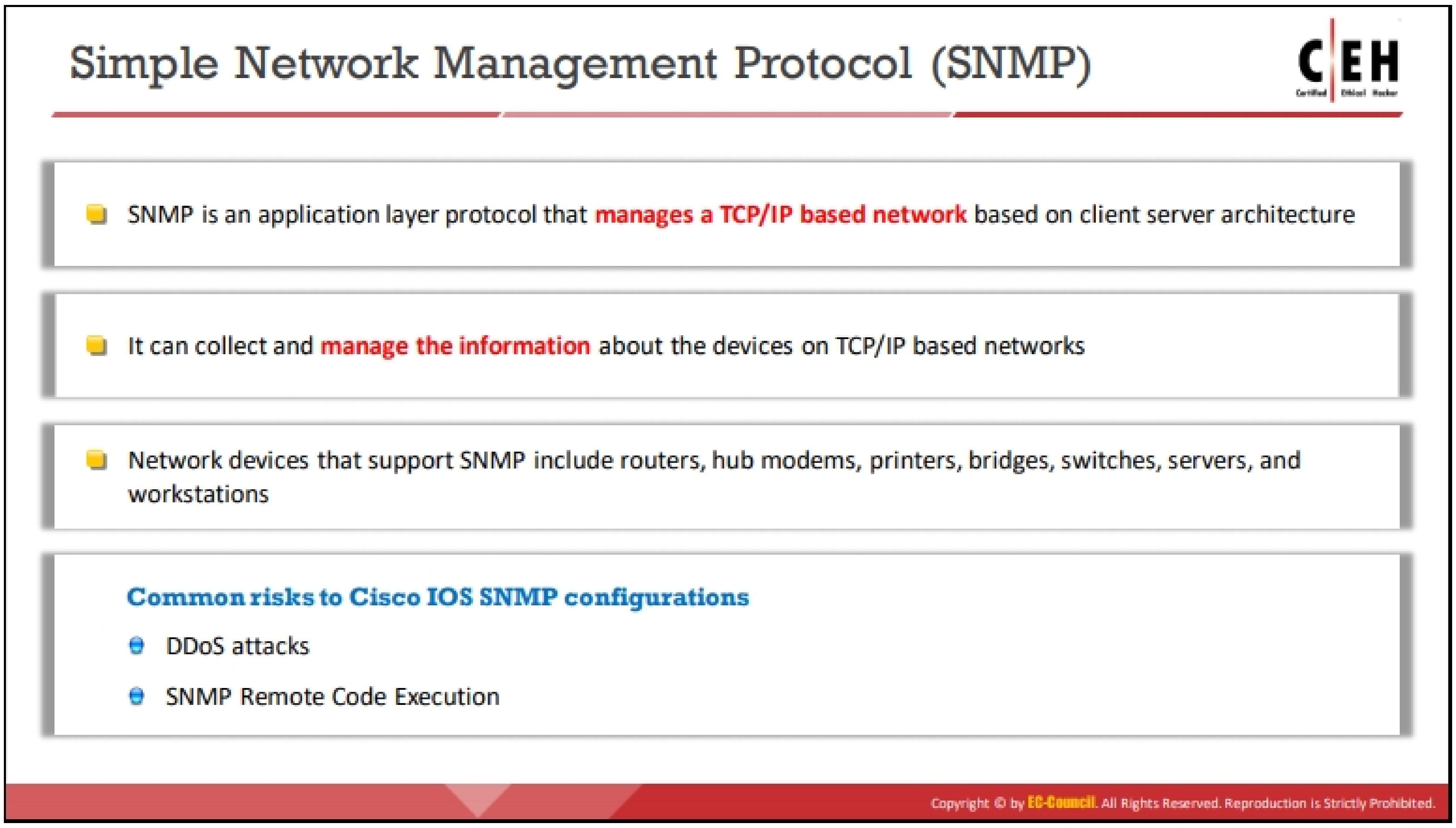


SOAP (Simple Object Access Protocol)

- The Simple Object Access Protocol (SOAP) is an **XML-Based messaging protocol** used to transmit data between computers
- It provides **data transport for web services** and is independent of both platform and language; SOAP can be used in any language
- It has three different characteristics: extensibility, neutrality, and independence
- It is **equivalent to RPC** (Remote Procedure Calls), which is used in technologies like DCOM and COBRA

Weaknesses:

- Statelessness
- Too much reliance on HTTP
- Slower than CORBA, RMI, or IIOP due to the lengthy XML format that it must follow and the parsing of the envelop that is required
- It depends on WSDL and does not have any standardized mechanism for dynamic discovery of the services



Simple Network Management Protocol (SNMP)

- SNMP is an application layer protocol that **manages a TCP/IP based network** based on client server architecture
- It can collect and **manage the information** about the devices on TCP/IP based networks
- Network devices that support SNMP include routers, hub modems, printers, bridges, switches, servers, and workstations

Common risks to Cisco IOS SNMP configurations

- DDoS attacks
- SNMP Remote Code Execution

Notes: ____

____

____

____

____

____

NTP (Network Time Protocol)

- NTP is used to **synchronize the clock times of computer** in a network

- The NTP client initiates a **time request exchange** with the NTP server

Features:

- Uses UTC as a reference time
- Highly scalable

Weaknesses :

- It is vulnerable to denial-of-service attacks and DDoS amplification attacks
- Intruders can intercept the packets between an authentic client and server
- Intruders can replay one or more packets

RPC (Remote Procedure Call)

- Remote Procedure Call (RPC) is a protocol that allows **inter-process communication** between two programs (client and server) without having to understand the network's details
- Some of the RPC services on Unix are the Network Information Service, Network File System, and Common Desktop Environment
- Some of the **recent RPC vulnerabilities** on Windows and Linux platform:
  - Microsoft Windows Remote Procedure Call Security Bypass Vulnerability
  - Microsoft RPC DCOM Interface Overflow
  - Microsoft Windows RPC CVE-2017-8461 Remote Code Execution Vulnerability
  - Multiple Linux Vendor rpc.statd Remote Format String Vulnerability
  - Port 111 rpcbind Vulnerability

Vulnerability Details : CVE-2017-8461

Notes: ____

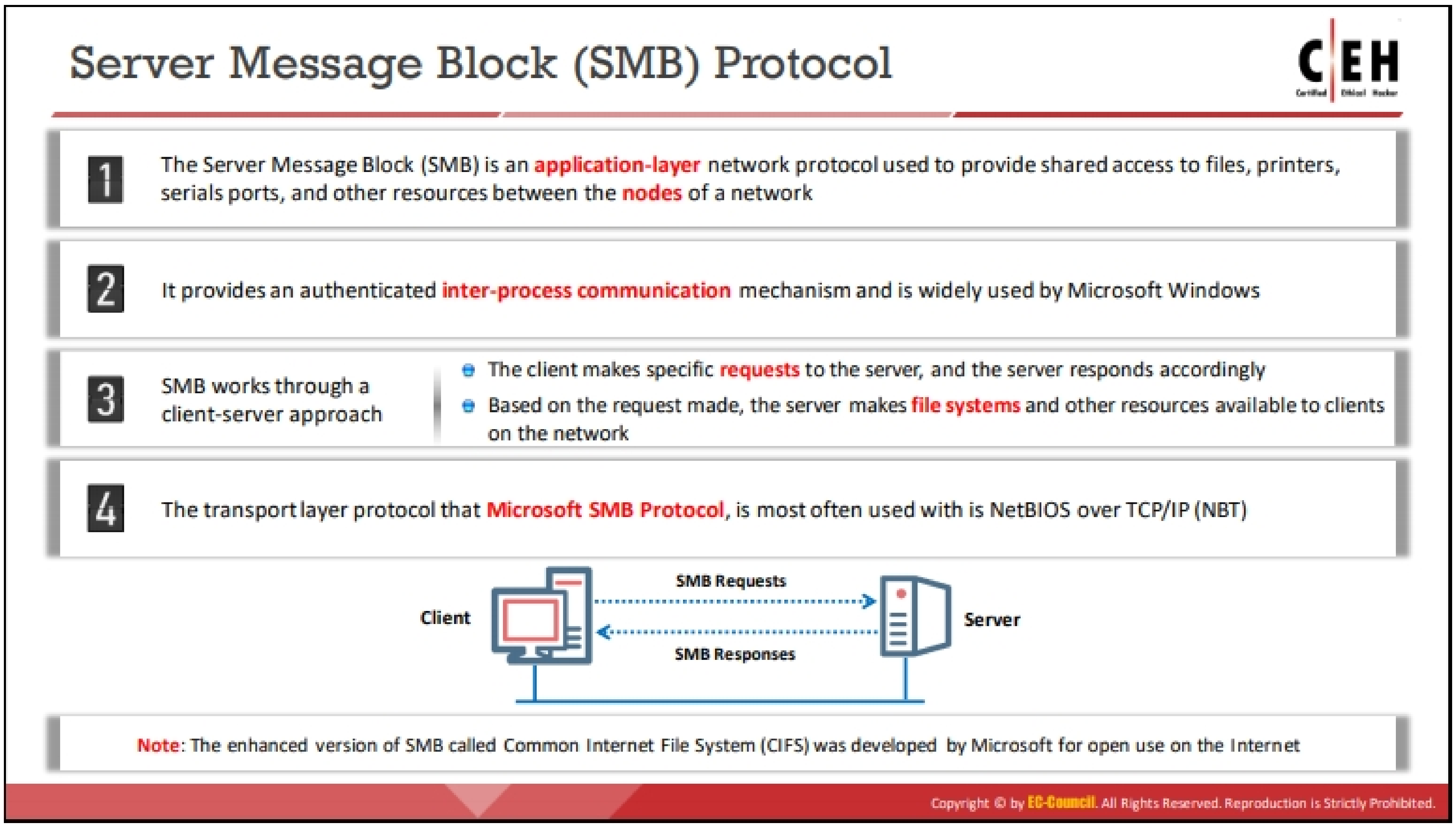
____

____

____

____

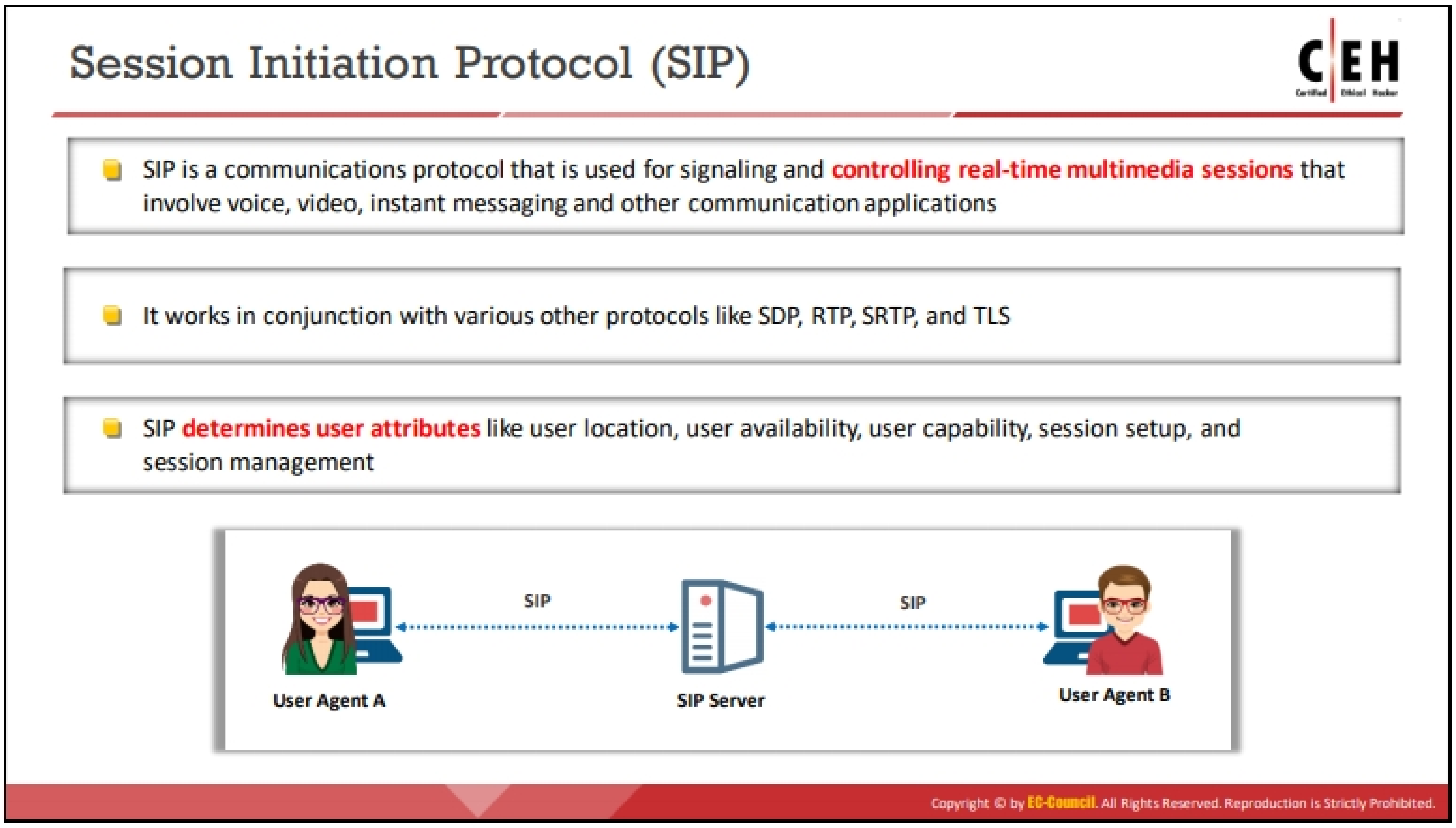
____



Server Message Block (SMB) Protocol

1. The Server Message Block (SMB) is an **application-layer** network protocol used to provide shared access to files, printers, serials ports, and other resources between the **nodes** of a network
2. It provides an authenticated **inter-process communication** mechanism and is widely used by Microsoft Windows
3. SMB works through a client-server approach
   - The client makes specific **requests** to the server, and the server responds accordingly
   - Based on the request made, the server makes **file systems** and other resources available to clients on the network
4. The transport layer protocol that **Microsoft SMB Protocol**, is most often used with is NetBIOS over TCP/IP (NBT)

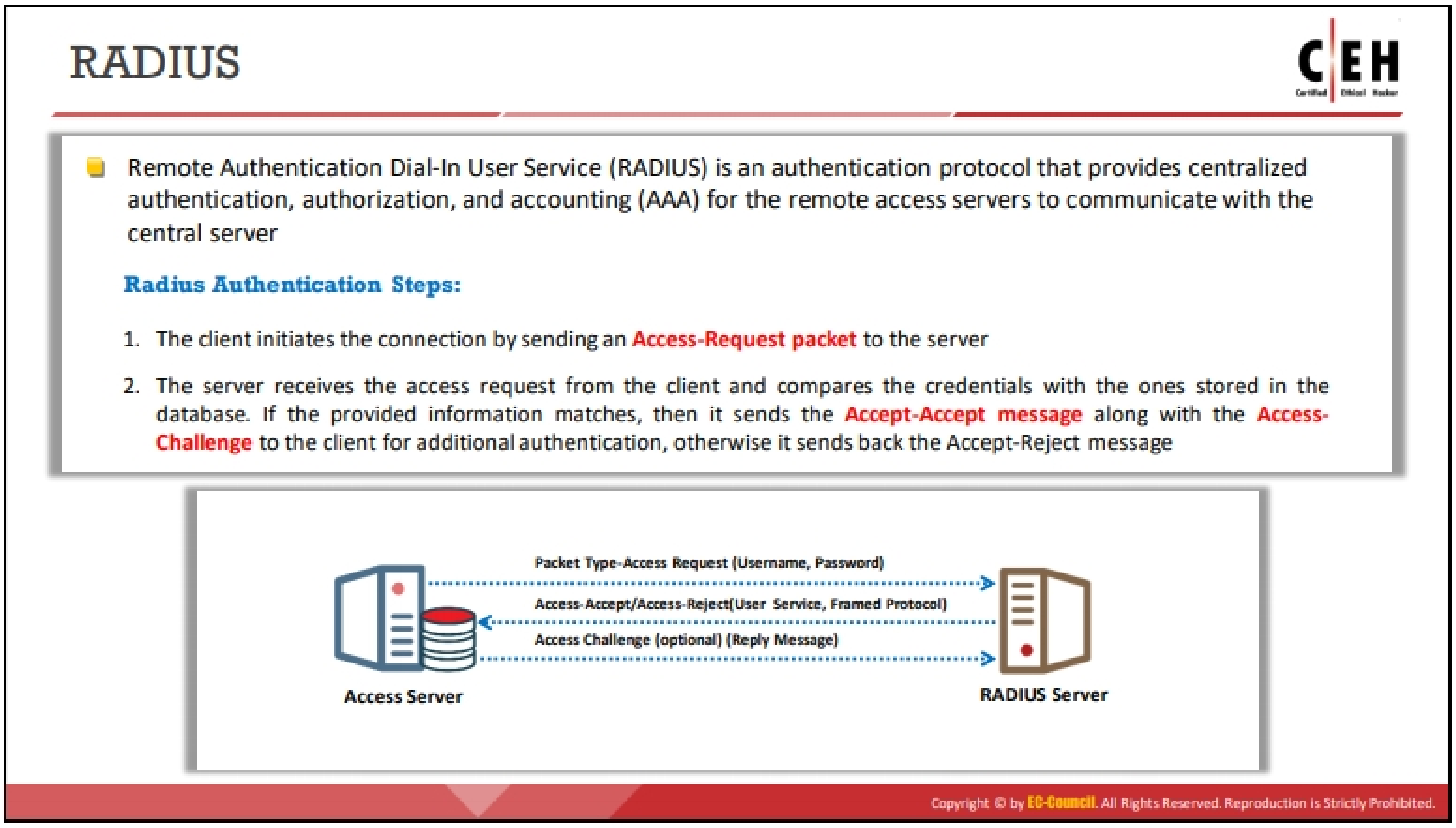
Note: The enhanced version of SMB called Common Internet File System (CIFS) was developed by Microsoft for open use on the Internet



Session Initiation Protocol (SIP)

- SIP is a communications protocol that is used for signaling and **controlling real-time multimedia sessions** that involve voice, video, instant messaging and other communication applications
- It works in conjunction with various other protocols like SDP, RTP, SRTP, and TLS
- SIP **determines user attributes** like user location, user availability, user capability, session setup, and session management

Notes:



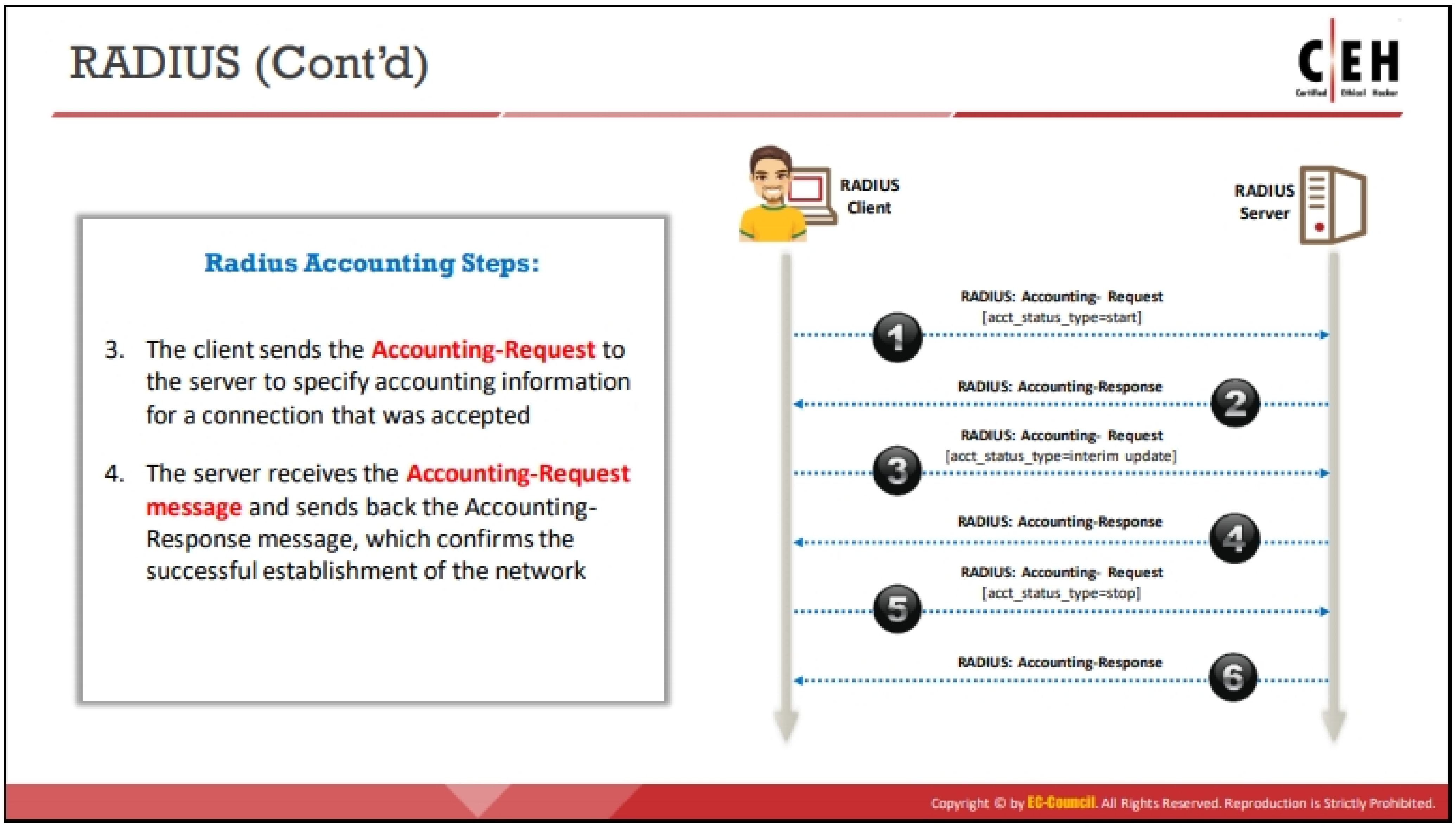
RADIUS

- Remote Authentication Dial-In User Service (RADIUS) is an authentication protocol that provides centralized authentication, authorization, and accounting (AAA) for the remote access servers to communicate with the central server

Radius Authentication Steps:

1. The client initiates the connection by sending an **Access-Request packet** to the server
2. The server receives the access request from the client and compares the credentials with the ones stored in the database. If the provided information matches, then it sends the **Accept-Accept message** along with the **Access-Challenge** to the client for additional authentication, otherwise it sends back the Accept-Reject message

Packet Type-Access Request (Username, Password)
Access-Accept/Access-Reject(User Service, Framed Protocol)
Access Challenge (optional) (Reply Message)
Access Server
RADIUS Server



RADIUS (Cont'd)

Radius Accounting Steps:

3. The client sends the **Accounting-Request** to the server to specify accounting information for a connection that was accepted
4. The server receives the **Accounting-Request message** and sends back the Accounting-Response message, which confirms the successful establishment of the network

RADIUS Client
RADIUS Server
1 RADIUS: Accounting- Request [acct_status_type=start]
2 RADIUS: Accounting-Response
3 RADIUS: Accounting- Request [acct_status_type=interim update]
4 RADIUS: Accounting-Response
5 RADIUS: Accounting- Request [acct_status_type=stop]
6 RADIUS: Accounting-Response

Notes: ____

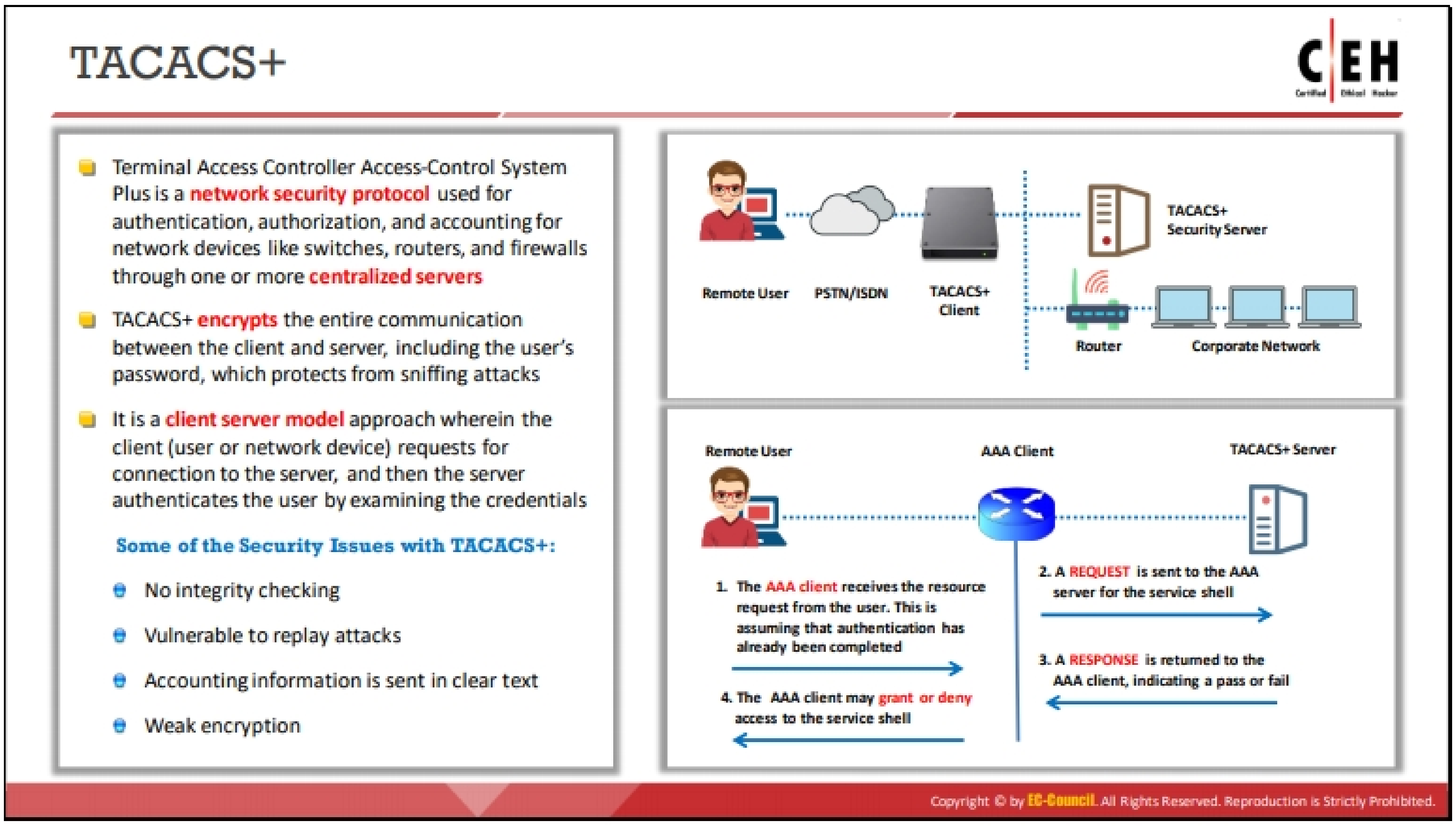
____

____

____

____

____



TACACS+

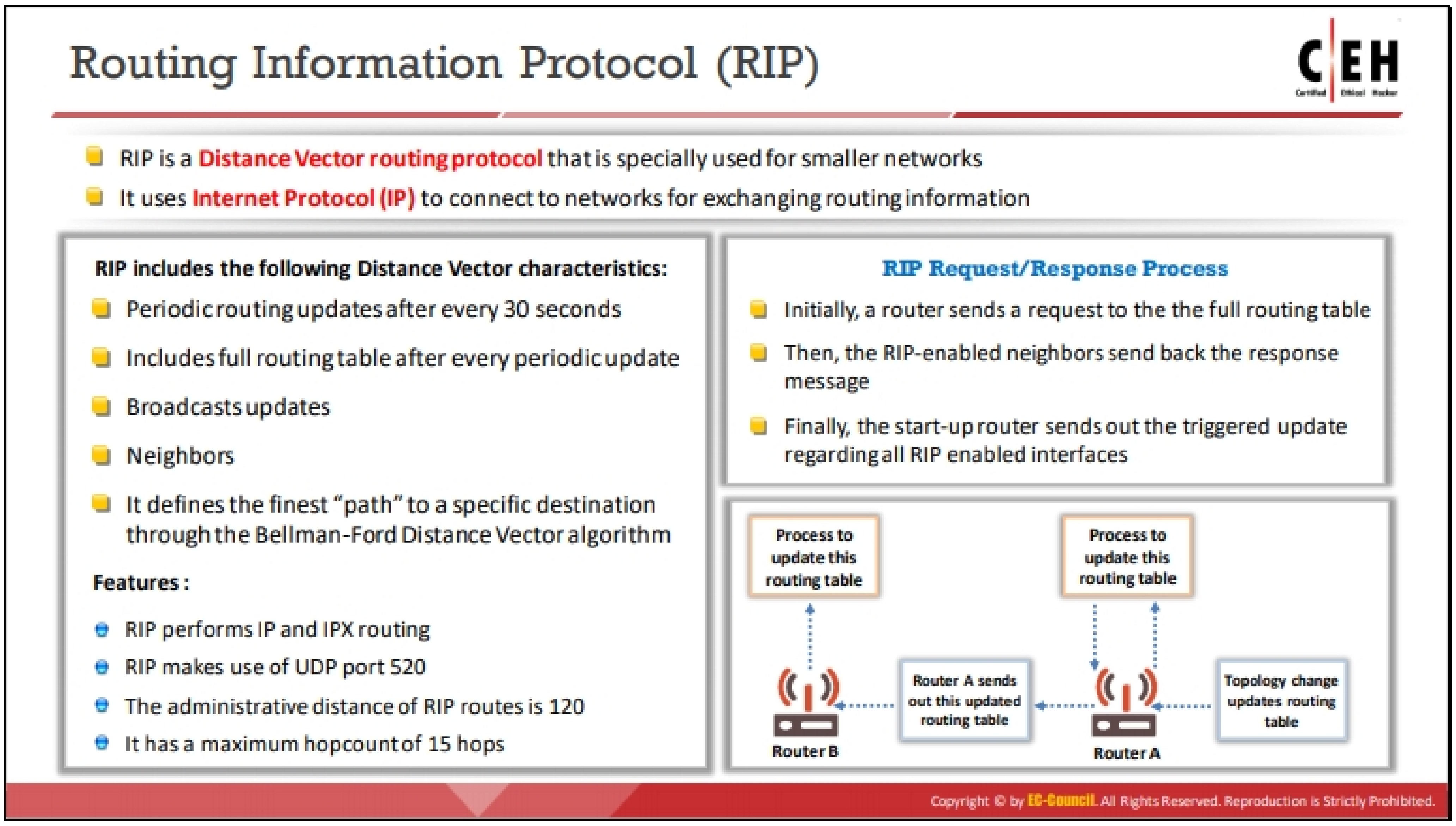
- Terminal Access Controller Access-Control System Plus is a **network security protocol** used for authentication, authorization, and accounting for network devices like switches, routers, and firewalls through one or more **centralized servers**
- TACACS+ **encrypts** the entire communication between the client and server, including the user's password, which protects from sniffing attacks
- It is a **client server model** approach wherein the client (user or network device) requests for connection to the server, and then the server authenticates the user by examining the credentials

Some of the Security Issues with TACACS+:

- No integrity checking
- Vulnerable to replay attacks
- Accounting information is sent in clear text
- Weak encryption

Remote User
PSTN/ISDN
TACACS+ Client
TACACS+ Security Server
Router
Corporate Network
Remote User
AAA Client
TACACS+ Server

1. The AAA client receives the resource request from the user. This is assuming that authentication has already been completed
2. A REQUEST is sent to the AAA server for the service shell
3. A RESPONSE is returned to the AAA client, indicating a pass or fail
4. The AAA client may grant or deny access to the service shell



Routing Information Protocol (RIP)

- RIP is a **Distance Vector routing protocol** that is specially used for smaller networks
- It uses **Internet Protocol (IP)** to connect to networks for exchanging routing information

RIP includes the following Distance Vector characteristics:

- Periodic routing updates after every 30 seconds
- Includes full routing table after every periodic update
- Broadcasts updates
- Neighbors
- It defines the finest "path" to a specific destination through the Bellman-Ford Distance Vector algorithm

Features :

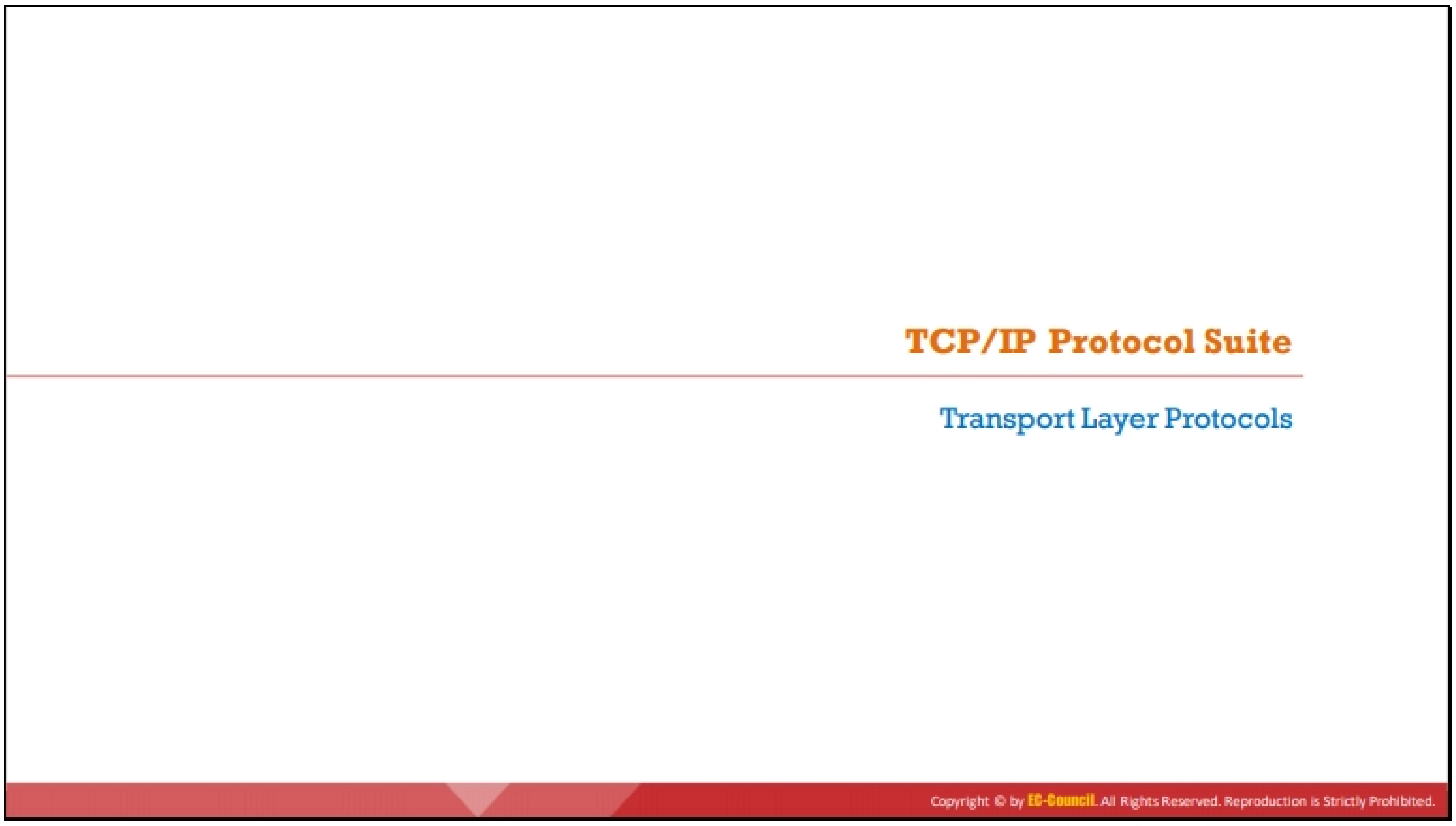
- RIP performs IP and IPX routing
- RIP makes use of UDP port 520
- The administrative distance of RIP routes is 120
- It has a maximum hopcount of 15 hops

RIP Request/Response Process

- Initially, a router sends a request to the the full routing table
- Then, the RIP-enabled neighbors send back the response message
- Finally, the start-up router sends out the triggered update regarding all RIP enabled interfaces

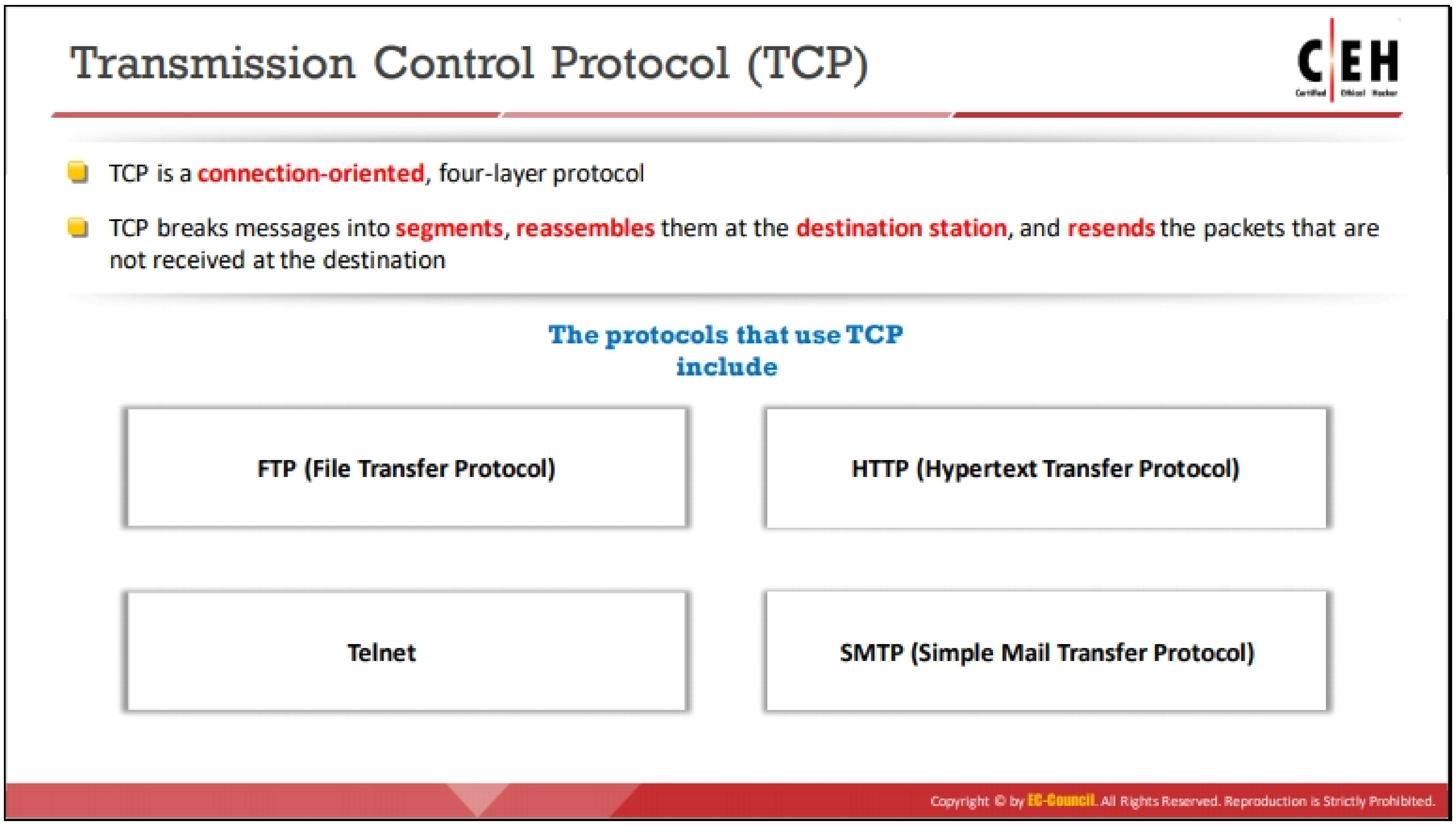
Process to update this routing table
Process to update this routing table
Router A sends out this updated routing table
Topology change updates routing table
Router B
Router A

Notes:



TCP/IP Protocol Suite

Transport Layer Protocols



Transmission Control Protocol (TCP)

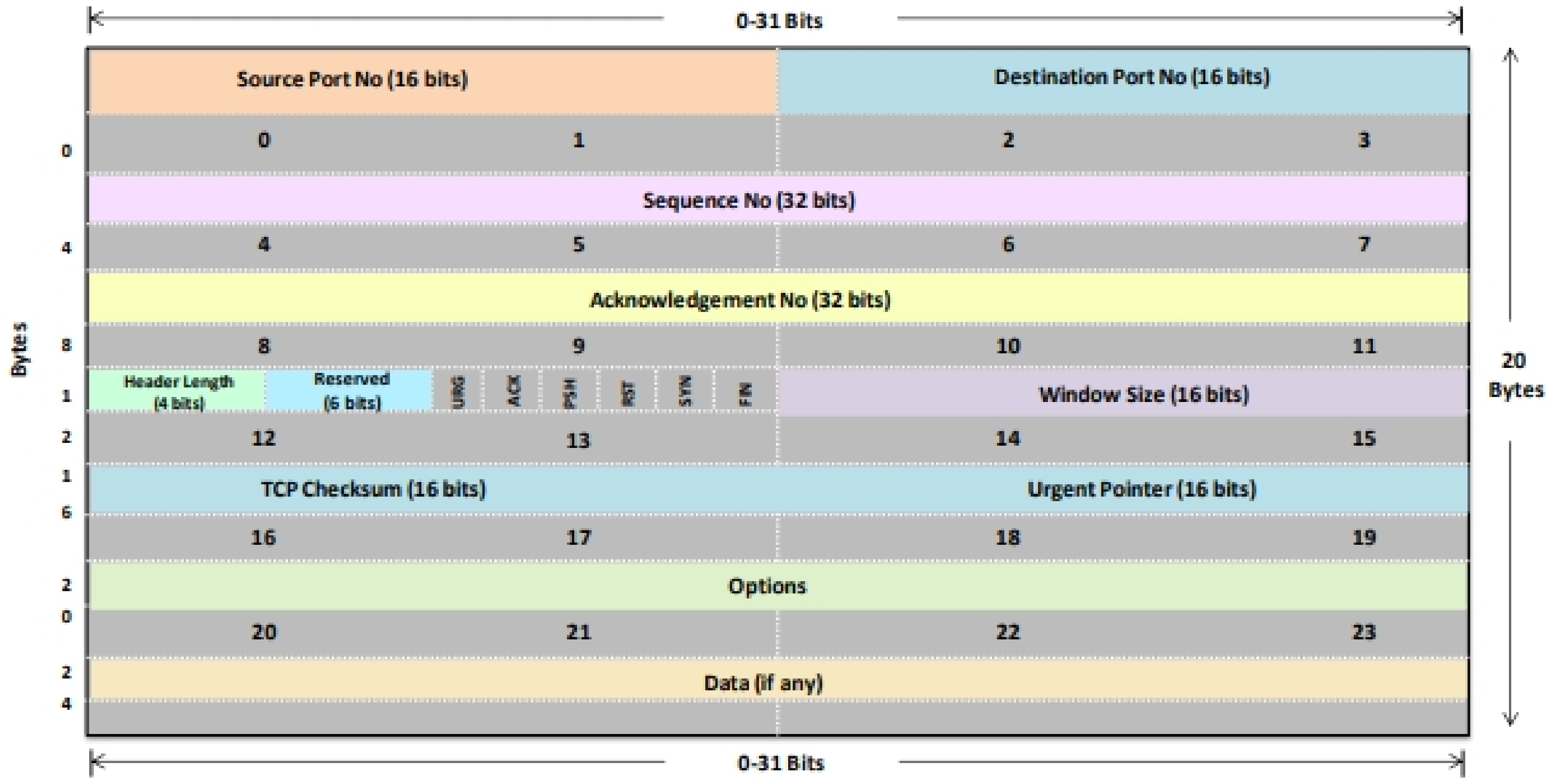
- TCP is a **connection-oriented**, four-layer protocol
- TCP breaks messages into **segments**, **reassembles** them at the **destination station**, and **resends** the packets that are not received at the destination

The protocols that use TCP include

FTP (File Transfer Protocol)	**HTTP (Hypertext Transfer Protocol)**
Telnet	**SMTP (Simple Mail Transfer Protocol)**

Notes:

TCP Header Format


0-31 Bits
Source Port No (16 bits)
Destination Port No (16 bits)
0
1
2
3
Sequence No (32 bits)
4
5
6
7
Acknowledgement No (32 bits)
8
9
10
11
Header Length (4 bits)
Reserved (6 bits)
URG
ACK
PSH
RST
SYN
FIN
Window Size (16 bits)
12
13
14
15
TCP Checksum (16 bits)
Urgent Pointer (16 bits)
16
17
18
19
Options
20
21
22
23
Data (if any)
0-31 Bits
Bytes
0
4
8
12
16
20
24
20 Bytes

TCP Services

1 **Simplex**

- Each flow has its own window size, **sequence** numbers, and **acknowledgment** numbers

2 **Half-duplex**

- Allows sending information in **both directions** between two nodes, but only one direction can be utilized at a time

3 **Full-duplex**

- Allows data flow in each direction, **independent** of the other direction
- Each flow has its own window size, **sequence** numbers, and **acknowledgment** numbers

Notes: ____

User Datagram Protocol (UDP)

- UDP is a connectionless transport protocol that exchanges datagrams without acknowledgments or guaranteed delivery
- It does not use **windowing** or **acknowledgments**, so reliability, if needed, is provided by application layer protocols

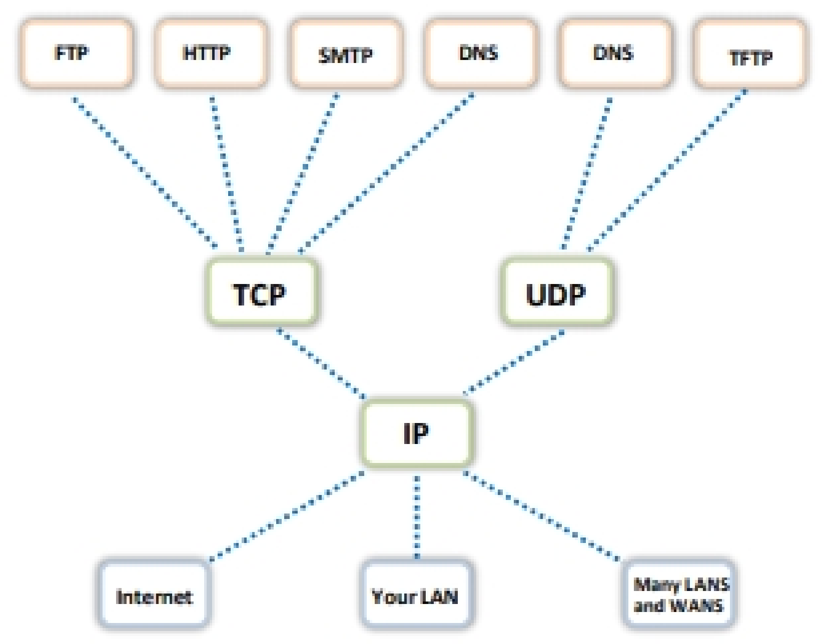
- The **protocols** that use UDP include:
  - TFTP (Trivial File Transfer Protocol)
  - SNMP (Simple Network Management Protocol)
  - DHCP (Dynamic Host Configuration Protocol)

UDP Segment Format

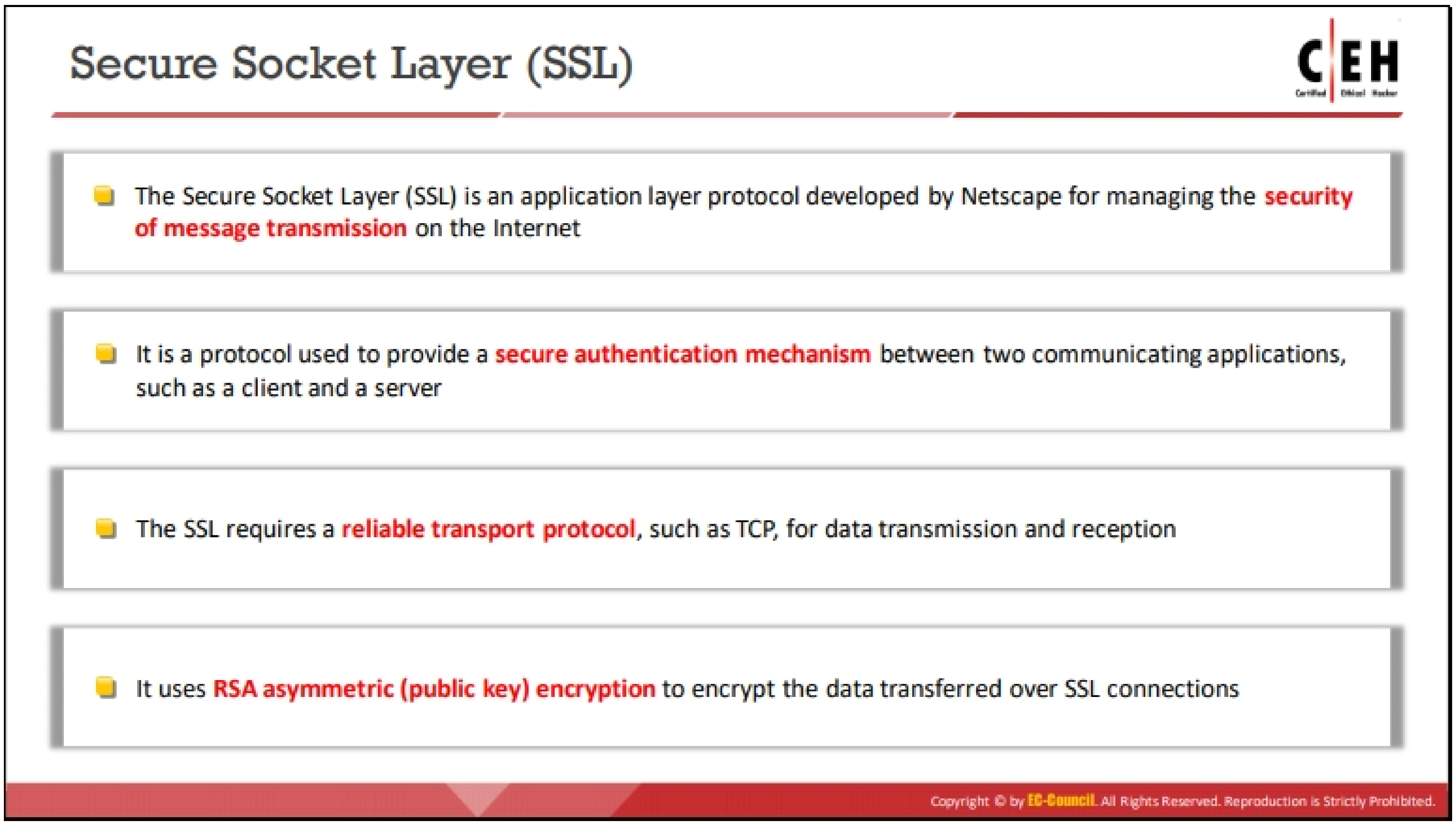
# of Bits	16	16	16	16	16
	Source Port	Destination Port	Length	Checksum	Data

UDP Operation

- UDP does not use windowing or acknowledgments, so application **layer** protocols are used for **error detection**
- The **Source Port** field is an optional field used only when information needs to be returned to the sending host
- When a **destination** router receives a routing update, it is not because the **source** router is making a request; therefore, nothing needs to be returned to the source
- In case of **RIP** updates only:
  - **BGP** uses **TCP**; **IGRP** is sent directly over **IP**
  - **EIGRP** and **OSPF** are also sent directly over IP with their own way of handling reliability

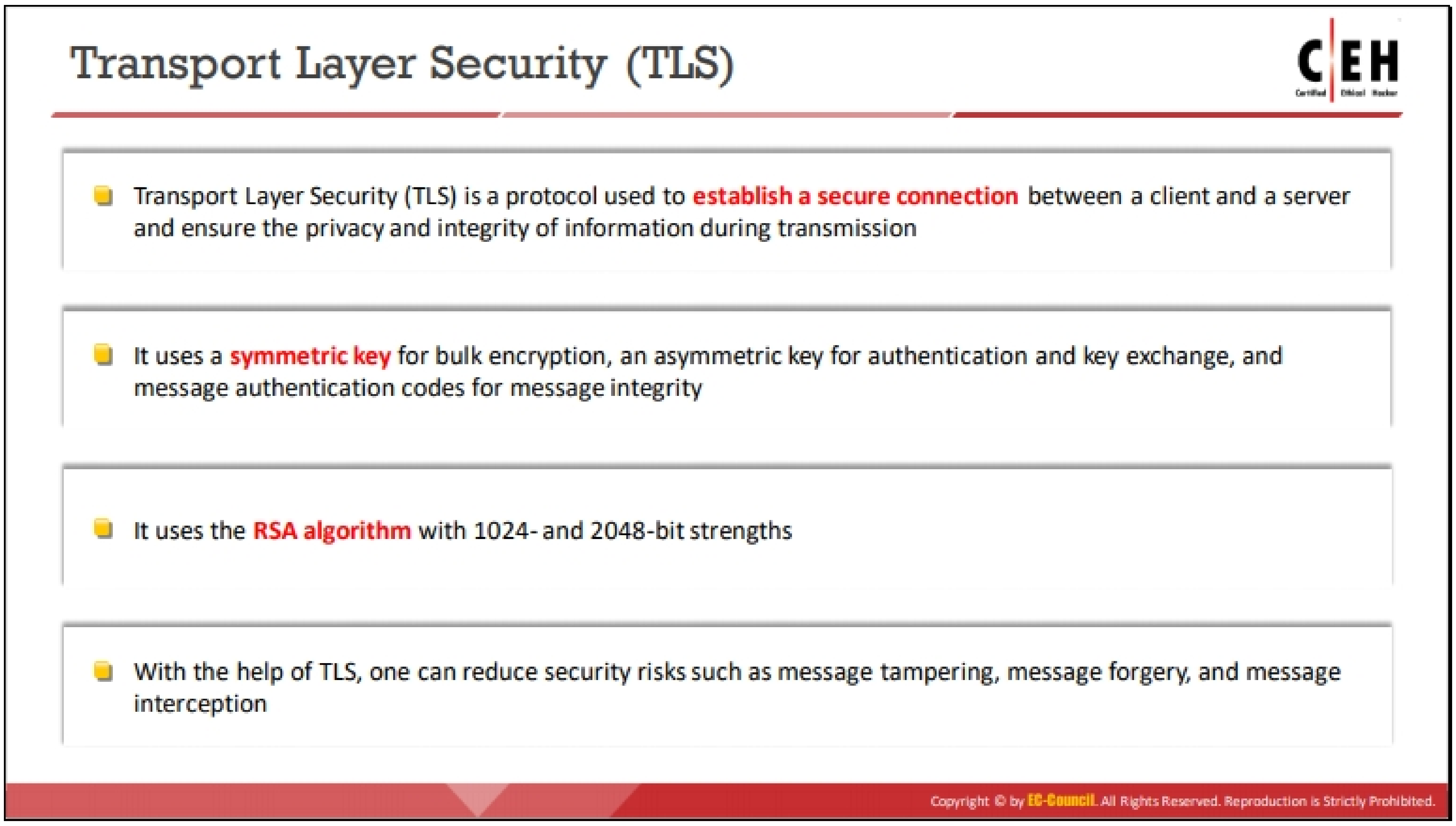


Notes: ____



Secure Socket Layer (SSL)

- The Secure Socket Layer (SSL) is an application layer protocol developed by Netscape for managing the **security of message transmission** on the Internet
- It is a protocol used to provide a **secure authentication mechanism** between two communicating applications, such as a client and a server
- The SSL requires a **reliable transport protocol**, such as TCP, for data transmission and reception
- It uses **RSA asymmetric (public key) encryption** to encrypt the data transferred over SSL connections



Transport Layer Security (TLS)

- Transport Layer Security (TLS) is a protocol used to **establish a secure connection** between a client and a server and ensure the privacy and integrity of information during transmission
- It uses a **symmetric key** for bulk encryption, an asymmetric key for authentication and key exchange, and message authentication codes for message integrity
- It uses the **RSA algorithm** with 1024- and 2048-bit strengths
- With the help of TLS, one can reduce security risks such as message tampering, message forgery, and message interception

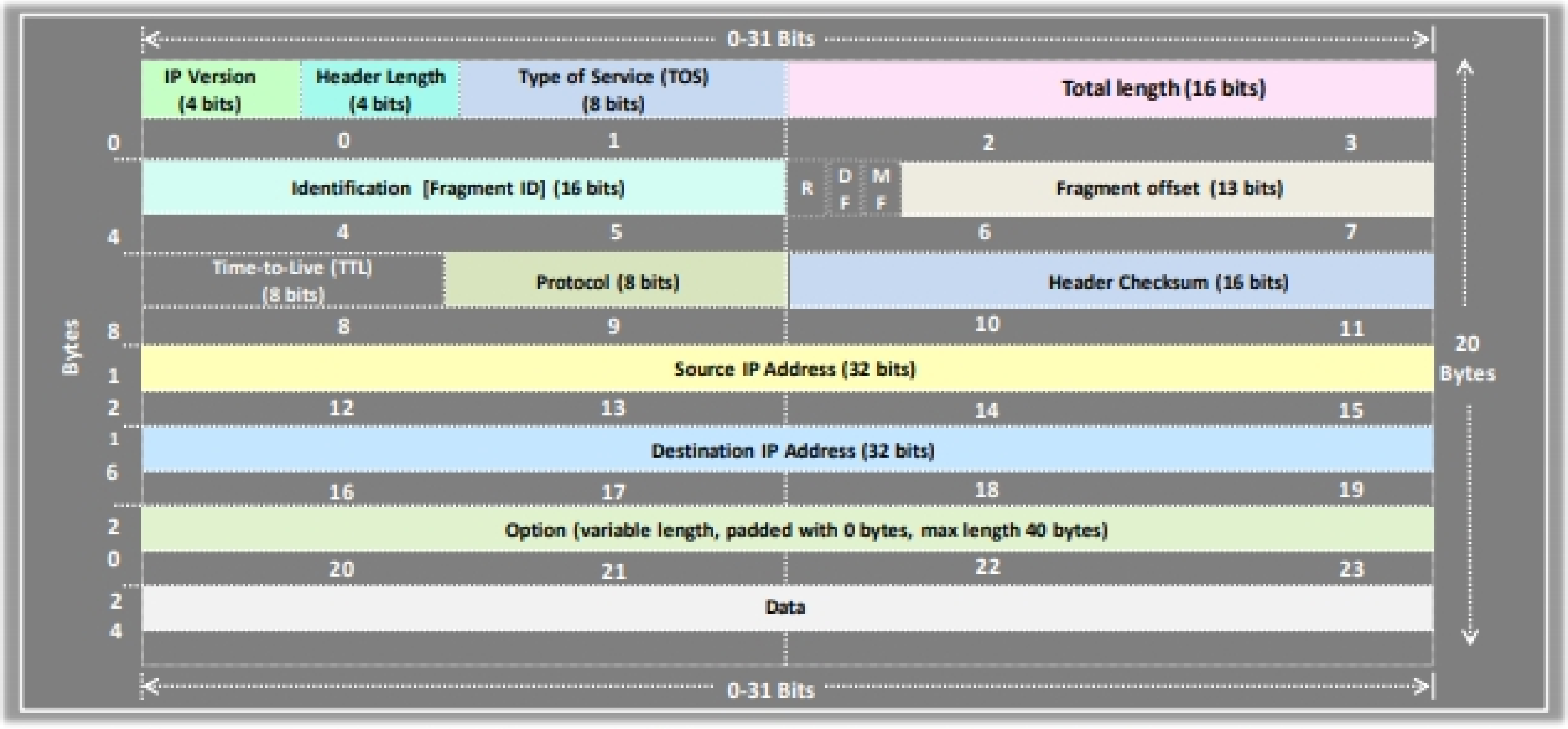
Notes: ____

TCP/IP Protocol Suite

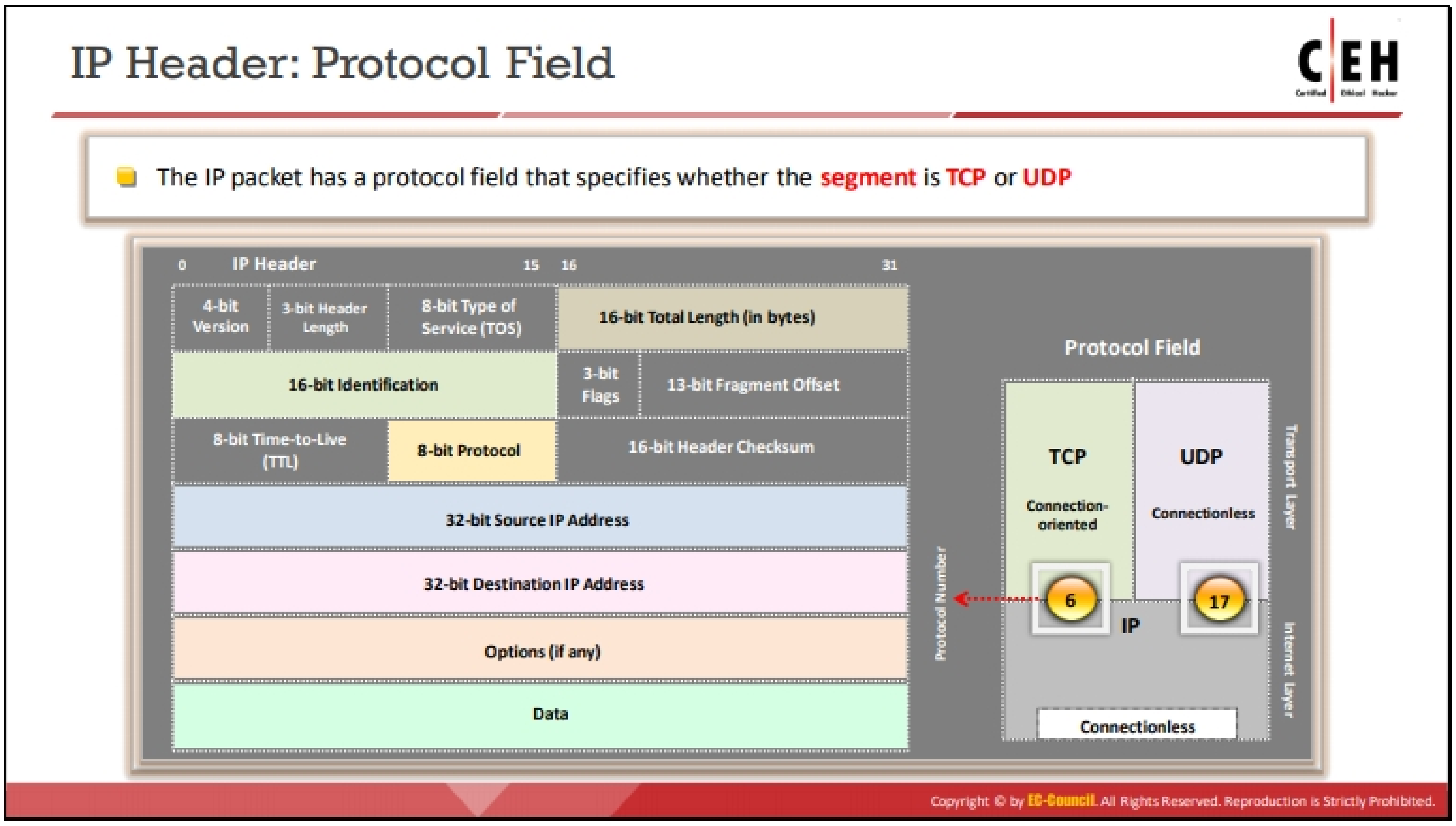
Internet Layer Protocols

Internet Protocol (IP)

- Internet Protocol (IP) is a **fundamental network layer protocol** in the TCP/IP protocol suite. It is primarily responsible for sending datagrams across network boundaries


0-31 Bits
IP Version (4 bits)
Header Length (4 bits)
Type of Service (TOS) (8 bits)
Total length (16 bits)
0
1
2
3
Identification [Fragment ID] (16 bits)
R
D F
M F
Fragment offset (13 bits)
4
5
6
7
Time-to-Live (TTL) (8 bits)
Protocol (8 bits)
Header Checksum (16 bits)
8
9
10
11
Source IP Address (32 bits)
12
13
14
15
Destination IP Address (32 bits)
16
17
18
19
Option (variable length, padded with 0 bytes, max length 40 bytes)
20
21
22
23
Data
0-31 Bits
Bytes
0
4
8
12
16
20
24
20 Bytes

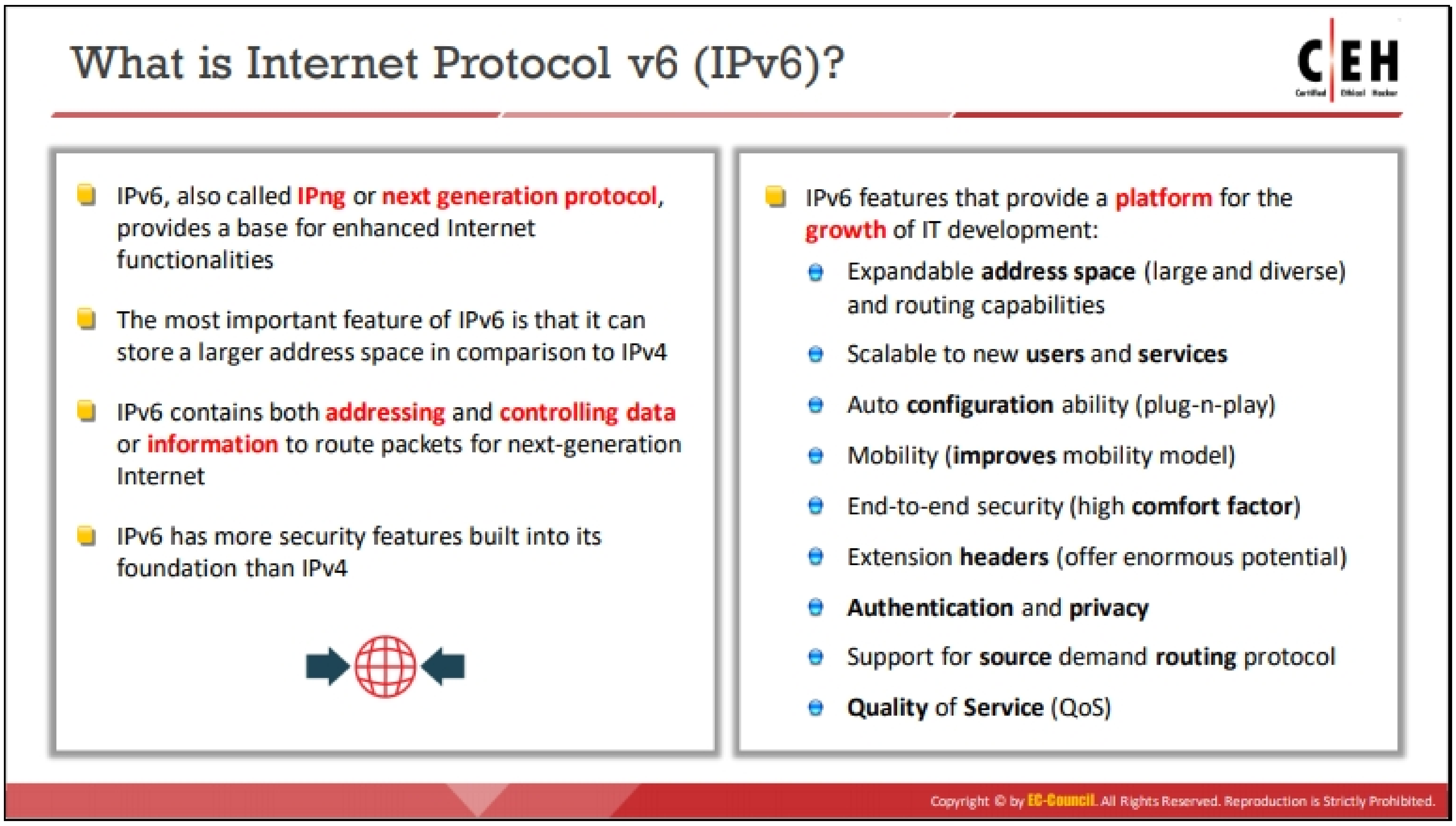
Notes:



IP Header: Protocol Field

- The IP packet has a protocol field that specifies whether the segment is TCP or UDP

0
IP Header
15
16
31
4-bit Version
3-bit Header Length
8-bit Type of Service (TOS)
16-bit Total Length (in bytes)
16-bit Identification
3-bit Flags
13-bit Fragment Offset
8-bit Time-to-Live (TTL)
8-bit Protocol
16-bit Header Checksum
32-bit Source IP Address
32-bit Destination IP Address
Options (if any)
Data
Protocol Field
TCP
Connection-oriented
UDP
Connectionless
Transport Layer
Protocol Number
6
17
IP
Internet Layer
Connectionless

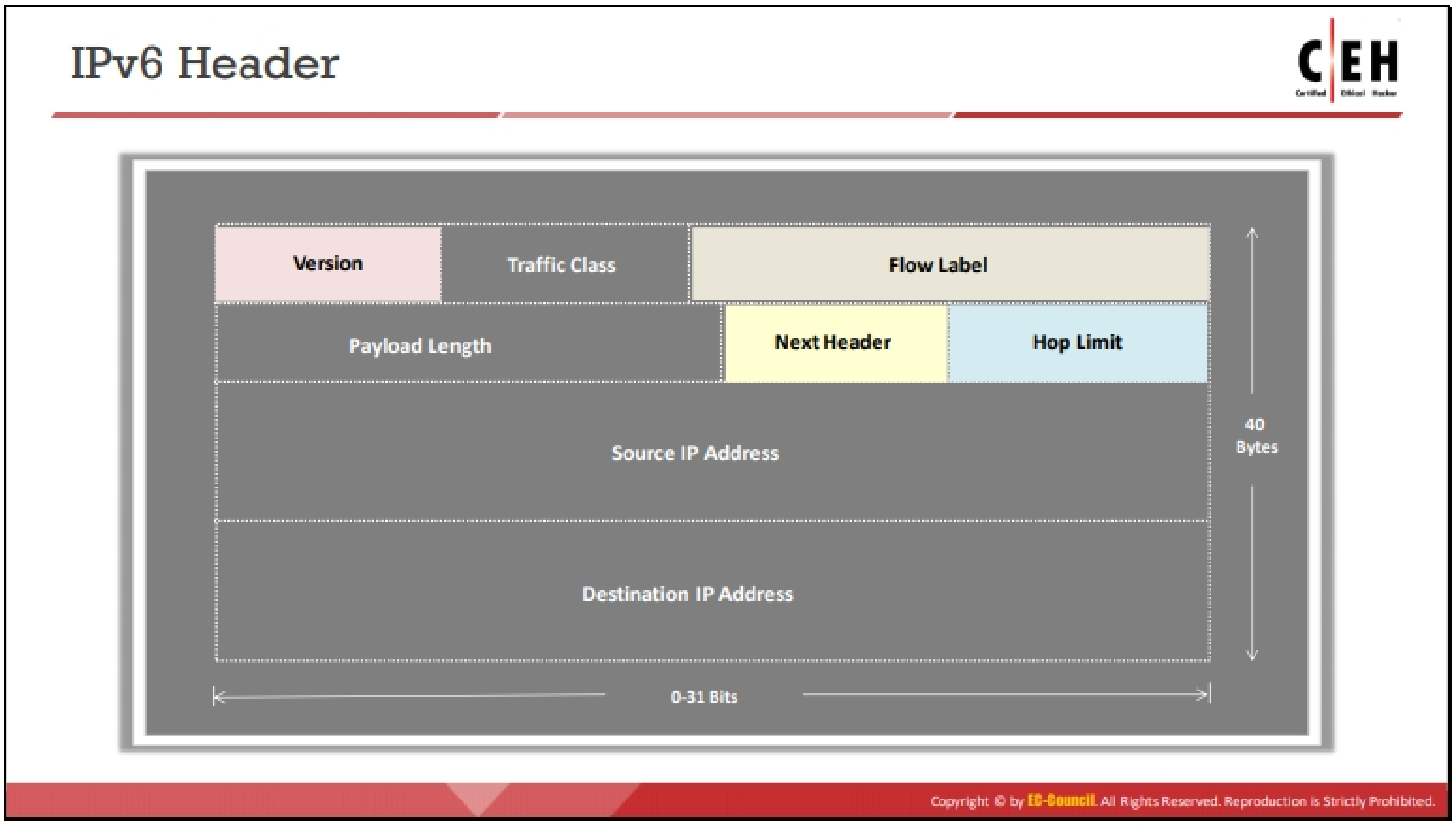


What is Internet Protocol v6 (IPv6)?

- IPv6, also called IPng or next generation protocol, provides a base for enhanced Internet functionalities
- The most important feature of IPv6 is that it can store a larger address space in comparison to IPv4
- IPv6 contains both addressing and controlling data or information to route packets for next-generation Internet
- IPv6 has more security features built into its foundation than IPv4

- IPv6 features that provide a platform for the growth of IT development:
  - Expandable **address space** (large and diverse) and routing capabilities
  - Scalable to new **users** and **services**
  - Auto **configuration** ability (plug-n-play)
  - Mobility (**improves** mobility model)
  - End-to-end security (high **comfort factor**)
  - Extension **headers** (offer enormous potential)
  - **Authentication** and **privacy**
  - Support for **source** demand **routing** protocol
  - **Quality** of **Service** (QoS)

Notes:

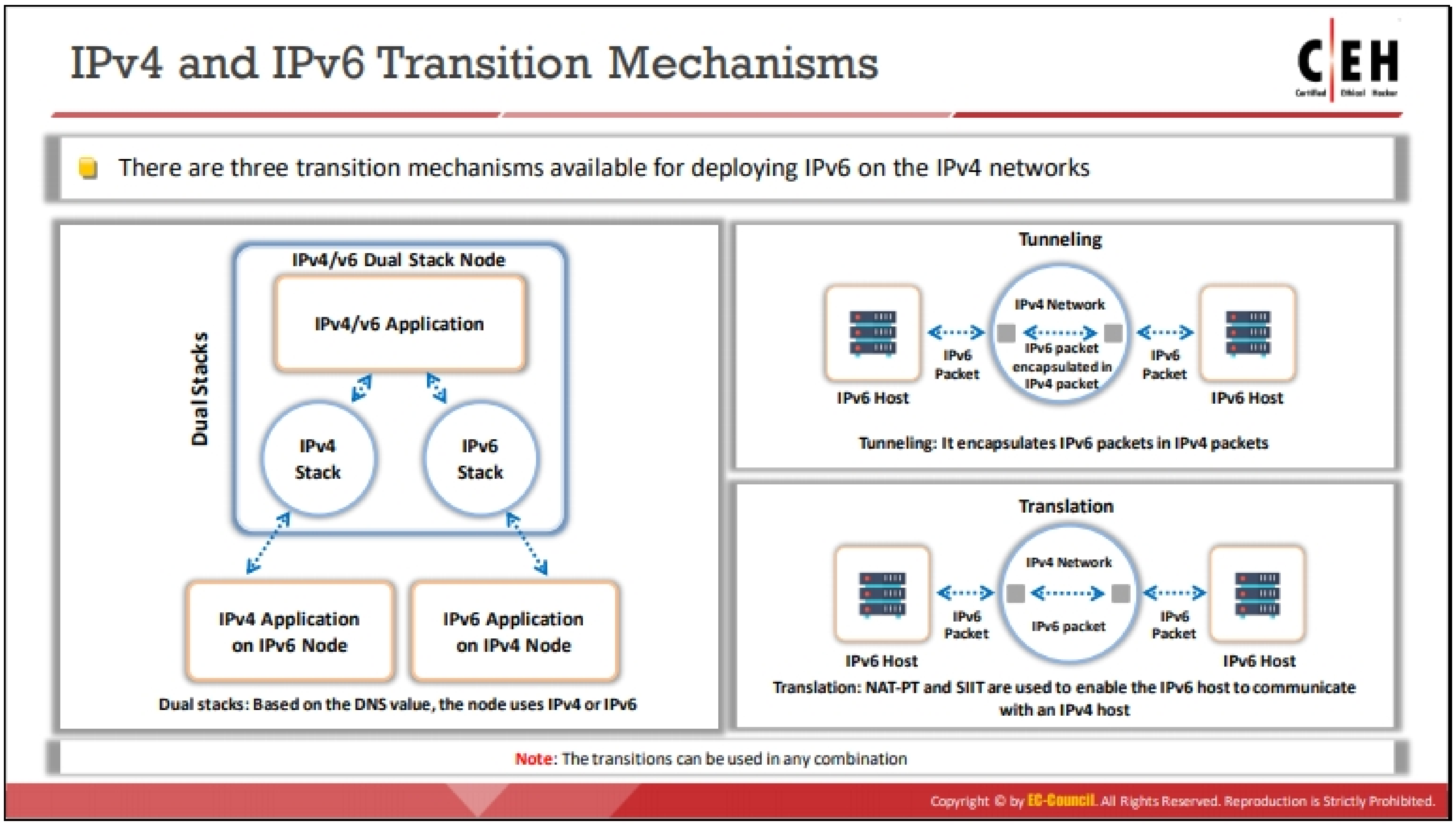


IPv6 Header

Version	Traffic Class	Flow Label
Payload Length	Next Header	Hop Limit
Source IP Address		
Destination IP Address		

0-31 Bits

40 Bytes



IPv4 and IPv6 Transition Mechanisms

- There are three transition mechanisms available for deploying IPv6 on the IPv4 networks

Dual Stacks

IPv4/v6 Dual Stack Node
IPv4/v6 Application
IPv4 Stack
IPv6 Stack
IPv4 Application on IPv6 Node
IPv6 Application on IPv4 Node

Dual stacks: Based on the DNS value, the node uses IPv4 or IPv6

Tunneling

IPv6 Host
IPv6 Packet
IPv4 Network
IPv6 packet encapsulated in IPv4 packet
IPv6 Packet
IPv6 Host

Tunneling: It encapsulates IPv6 packets in IPv4 packets

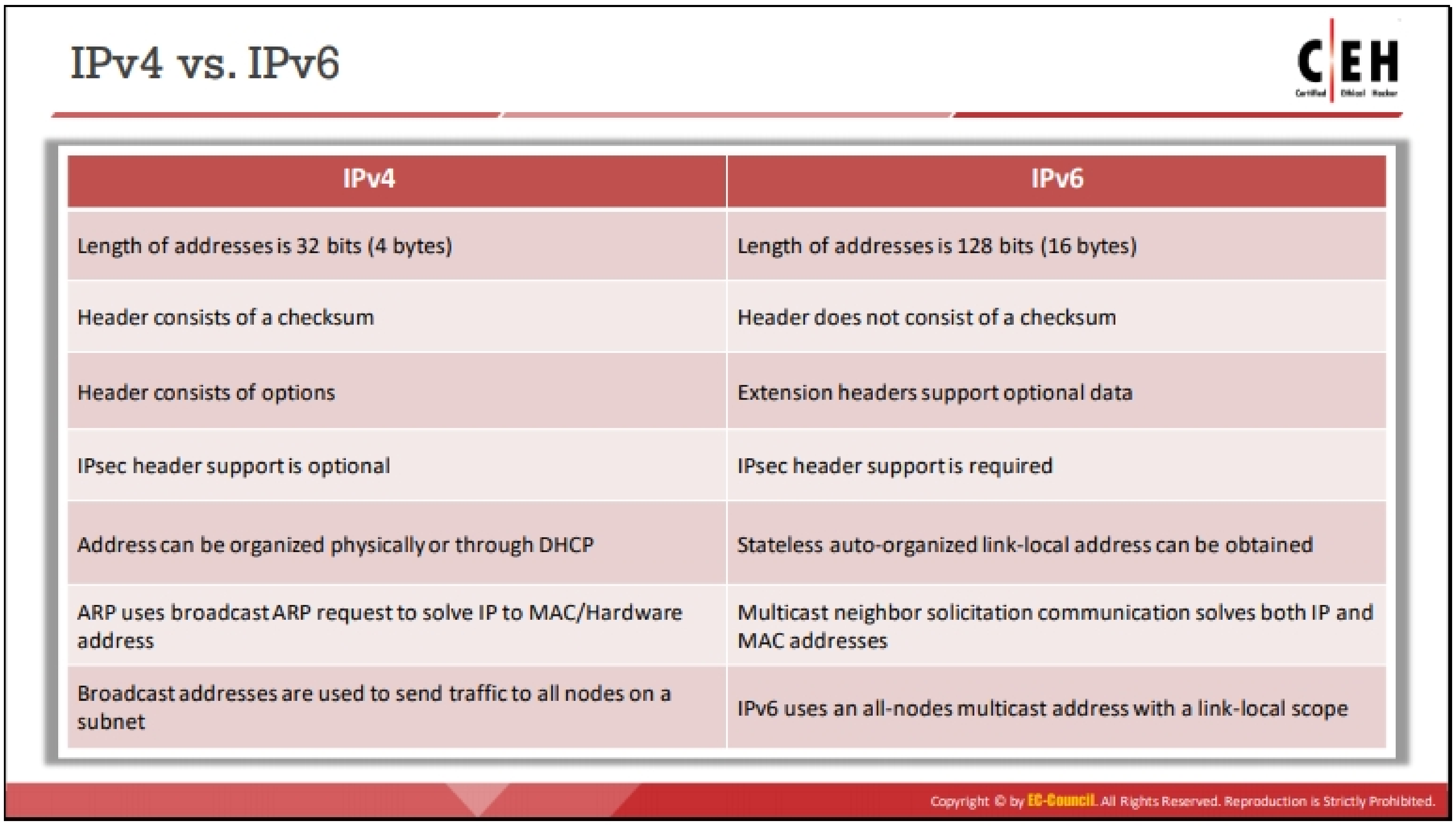
Translation

IPv6 Host
IPv6 Packet
IPv4 Network
IPv6 packet
IPv6 Packet
IPv6 Host

Translation: NAT-PT and SIIT are used to enable the IPv6 host to communicate with an IPv4 host

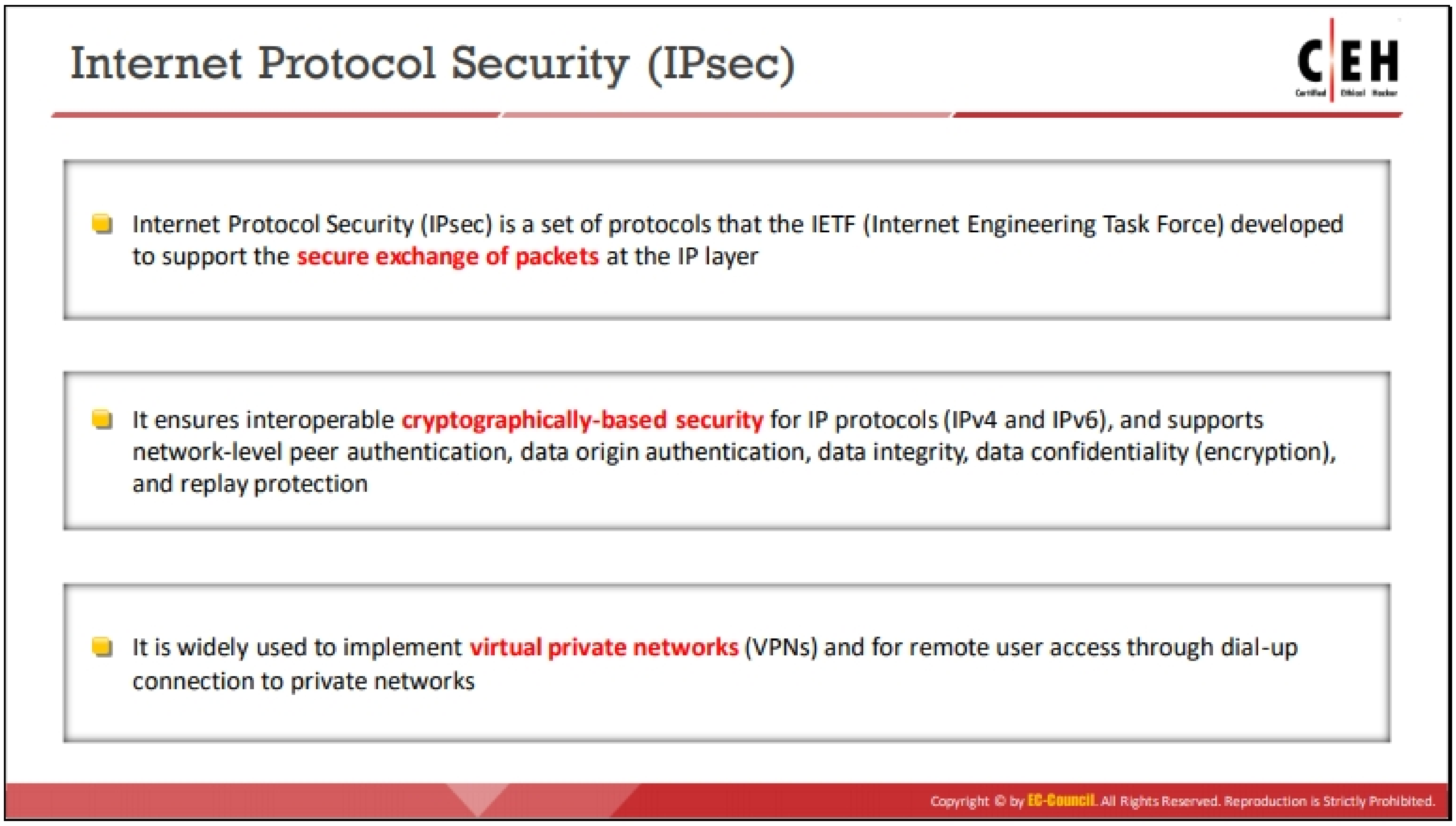
Note: The transitions can be used in any combination

Notes:



IPv4 vs. IPv6

IPv4	IPv6
Length of addresses is 32 bits (4 bytes)	Length of addresses is 128 bits (16 bytes)
Header consists of a checksum	Header does not consist of a checksum
Header consists of options	Extension headers support optional data
IPsec header support is optional	IPsec header support is required
Address can be organized physically or through DHCP	Stateless auto-organized link-local address can be obtained
ARP uses broadcast ARP request to solve IP to MAC/Hardware address	Multicast neighbor solicitation communication solves both IP and MAC addresses
Broadcast addresses are used to send traffic to all nodes on a subnet	IPv6 uses an all-nodes multicast address with a link-local scope



Internet Protocol Security (IPsec)

- Internet Protocol Security (IPsec) is a set of protocols that the IETF (Internet Engineering Task Force) developed to support the **secure exchange of packets** at the IP layer
- It ensures interoperable **cryptographically-based security** for IP protocols (IPv4 and IPv6), and supports network-level peer authentication, data origin authentication, data integrity, data confidentiality (encryption), and replay protection
- It is widely used to implement **virtual private networks** (VPNs) and for remote user access through dial-up connection to private networks

Notes: ____

Internet Control Message Protocol (ICMP)

- IP is an unreliable method for the delivery of network data
- It does not notify the sender of **failed data transmission**
- Internet Control Message Protocol (ICMP) is the component of the TCP/IP protocol stack that addresses this basic limitation of IP
- ICMP does not overcome the **unreliability issues in IP**
- Reliability, if required, must be provided by upper-layer protocols (TCP or the application)

Error Reporting and Correction

- When datagram delivery errors occur, **ICMP reports** the following errors back to the source of the datagram:

Workstation 1 sends a datagram to Workstation 6

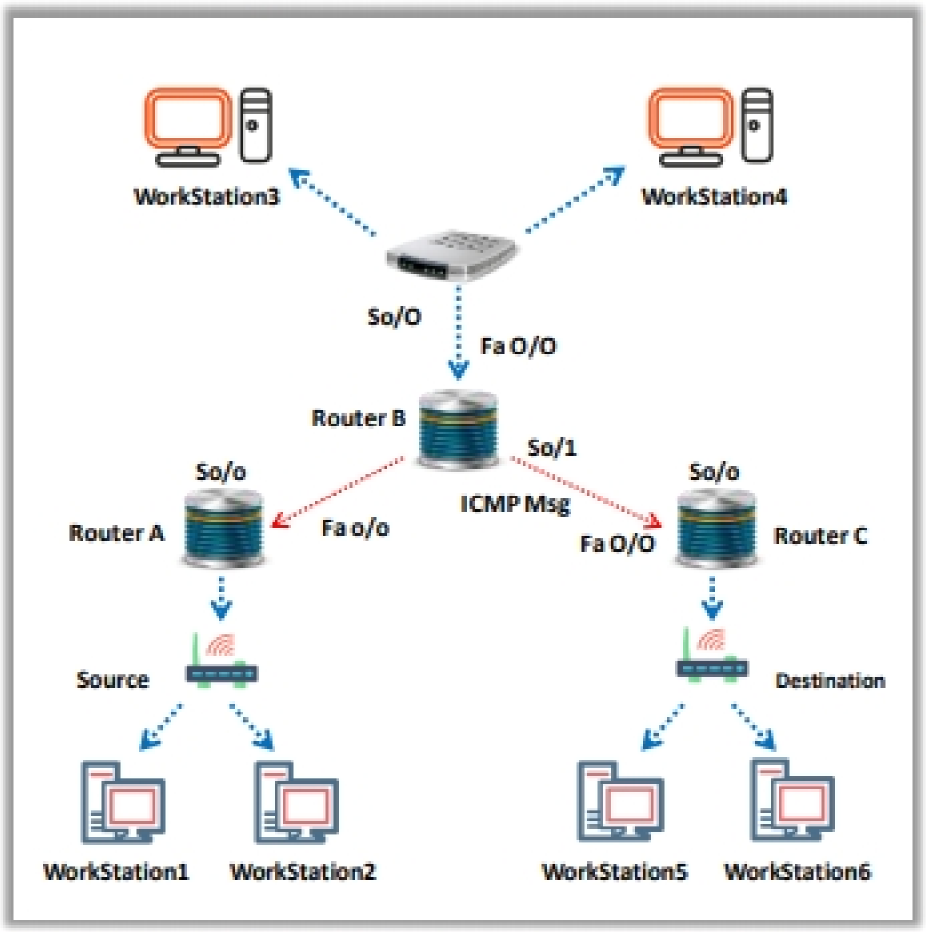
Fa0/0 on Router C goes down

Router C then utilizes ICMP to send a message indicating that the datagram could not be delivered back to Workstation 1

ICMP does not correct the encountered network problem

Router C knows only the source and destination IP addresses of the datagram

ICMP reports on the status of the delivered packet only to the source device


WorkStation3
WorkStation4
So/O
Fa O/O
Router B
So/1
So/o
So/o
Router A
Fa o/o
ICMP Msg
Fa O/O
Router C
Source
Destination
WorkStation1
WorkStation2
WorkStation5
WorkStation6

Notes: ____

____

____

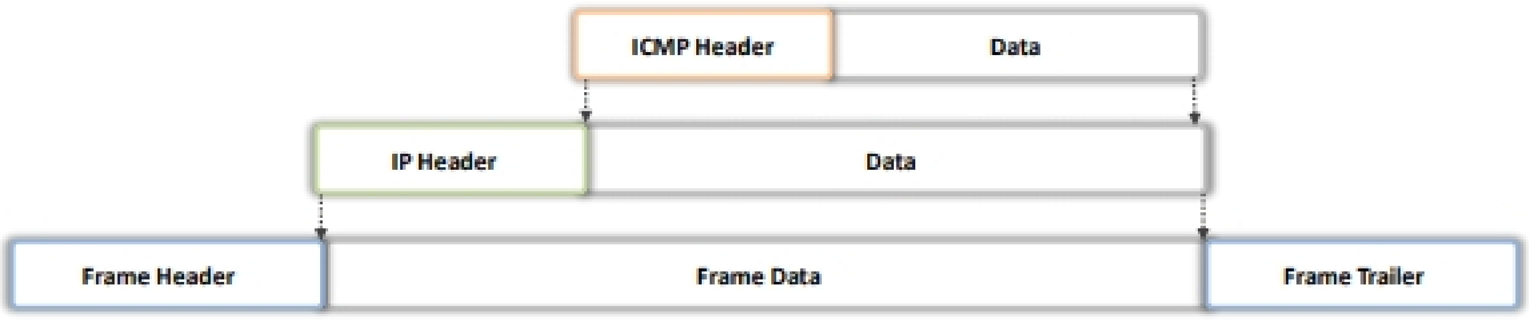
____

____

____

ICMP Message Delivery

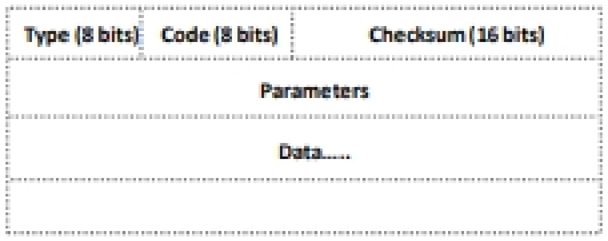
- ICMP messages are encapsulated into the **datagram**
- Encapsulation uses the same technique IP uses to **deliver data**, which is subject to the same delivery failures as any IP packet
- This creates a scenario where error reports could generate more error reports
- This causes increased congestion within an **already ailing network**
- Errors created by ICMP messages do not generate their **own ICMP messages**
- It is possible to have a datagram delivery error that is never reported back to the **sender of the data**



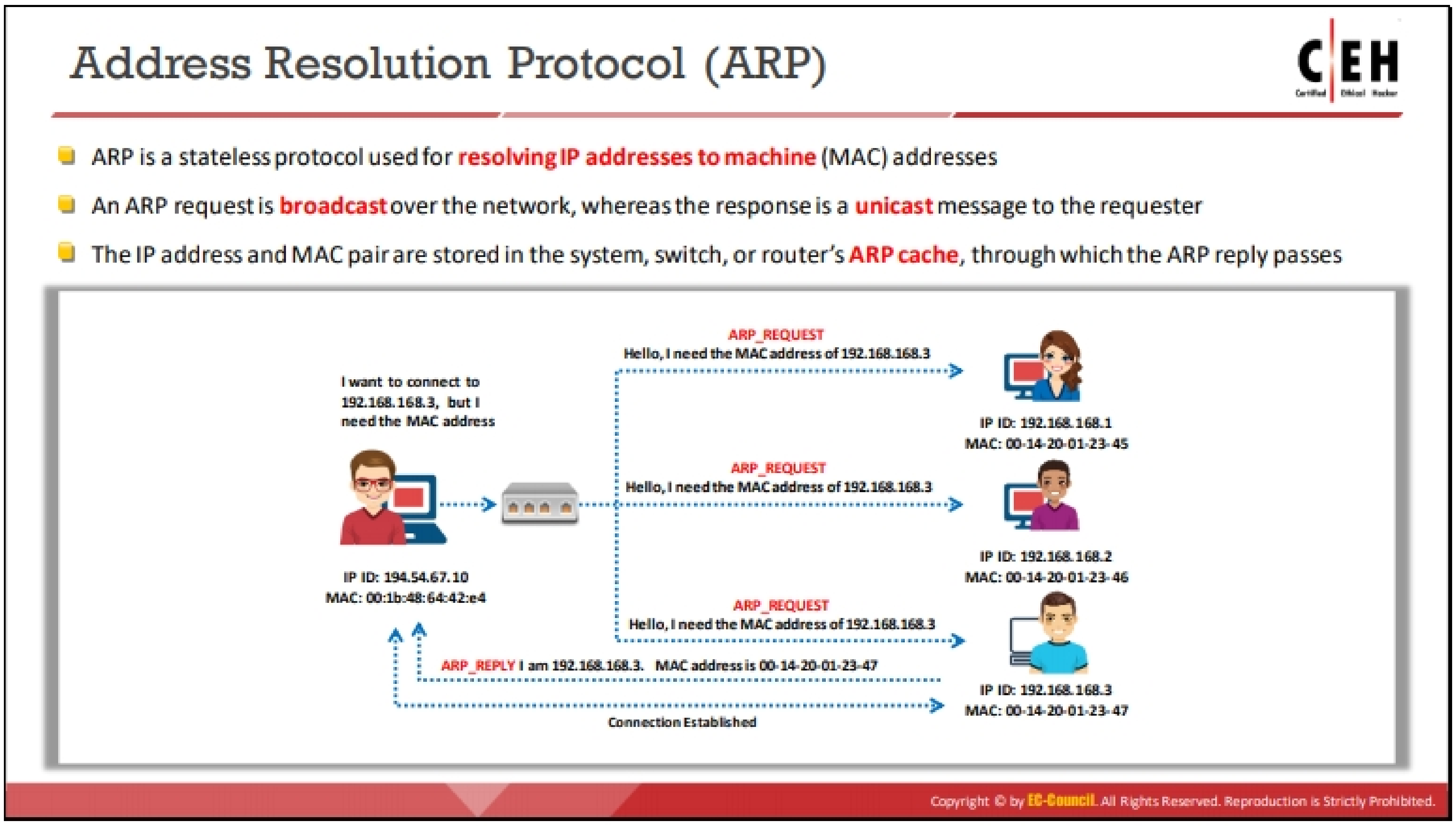
Format of an ICMP Message

```
Type      Name
----      -------------------------
  0       Echo Reply
  1       Unassigned
  2       Unassigned
  3       Destination Unreachable
  4       Source Quench
  5       Redirect
  6       Alternate Host Address
  7       Unassigned
  8       Echo
  9       Router Advertisement
 10       Router Solicitation
 11       Time Exceeded
 12       Parameter Problem
 13       Timestamp
 14       Timestamp Reply
 15       Information Request
 16       Information Reply
 17       Address Mask Request
 18       Address Mask Reply
 19       Reserved (for Security)
 20-29    Reserved (for Robustness Experiment)
 30       Traceroute
 31       Datagram Conversion Error
 32       Mobile Host Redirect
 33       IPv6 Where-Are-You
 34       IPv6 I-Am-Here
 35       Mobile Registration Request
 36       Mobile Registration Reply
 37       Domain Name Request
 38       Domain Name Reply
 39       SKIP
 40       Photuris
 41-255   Reserved
```

```
Code Field

Type 3: Destination Unreachable

Codes
0  Net Unreachable
1  Host Unreachable
2  Protocol Unreachable
3  Port Unreachable
4  Fragmentation Needed and Don't Fragment was Set
5  Source Route Failed
6  Destination Network Unknown
7  Destination Host Unknown
8  Source Host Isolated
9  Communication with Destination Network is Administratively Prohibited
10  Communication with Destination Host is Administratively Prohibited
11  Destination Network Unreachable for Type of Service
12  Destination Host Unreachable for Type of Service
13  Communication Administratively Prohibited
14  Host Precedence Violation
15  Precedence cutoff in effect
```



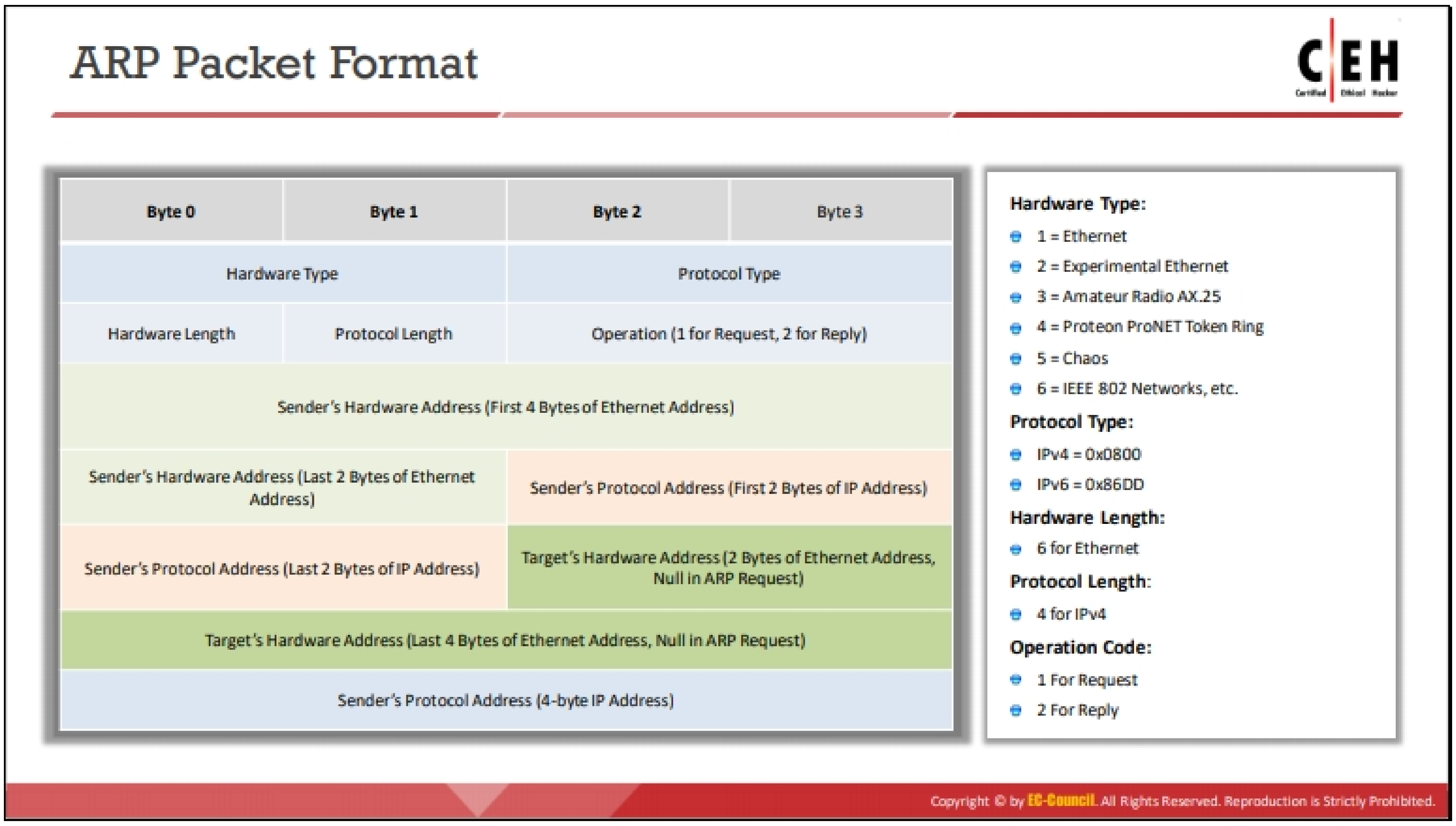
Notes: ____



Address Resolution Protocol (ARP)

- ARP is a stateless protocol used for **resolving IP addresses to machine** (MAC) addresses
- An ARP request is **broadcast** over the network, whereas the response is a **unicast** message to the requester
- The IP address and MAC pair are stored in the system, switch, or router's **ARP cache**, through which the ARP reply passes

I want to connect to 192.168.168.3, but I need the MAC address
IP ID: 194.54.67.10
MAC: 00:1b:48:64:42:e4
ARP_REQUEST
Hello, I need the MAC address of 192.168.168.3
IP ID: 192.168.168.1
MAC: 00-14-20-01-23-45
ARP_REQUEST
Hello, I need the MAC address of 192.168.168.3
IP ID: 192.168.168.2
MAC: 00-14-20-01-23-46
ARP_REQUEST
Hello, I need the MAC address of 192.168.168.3
ARP_REPLY I am 192.168.168.3. MAC address is 00-14-20-01-23-47
IP ID: 192.168.168.3
MAC: 00-14-20-01-23-47
Connection Established



ARP Packet Format

Byte 0	Byte 1	Byte 2	Byte 3
Hardware Type		Protocol Type	
Hardware Length	Protocol Length	Operation (1 for Request, 2 for Reply)	
Sender's Hardware Address (First 4 Bytes of Ethernet Address)			
Sender's Hardware Address (Last 2 Bytes of Ethernet Address)		Sender's Protocol Address (First 2 Bytes of IP Address)	
Sender's Protocol Address (Last 2 Bytes of IP Address)		Target's Hardware Address (2 Bytes of Ethernet Address, Null in ARP Request)	
Target's Hardware Address (Last 4 Bytes of Ethernet Address, Null in ARP Request)			
Sender's Protocol Address (4-byte IP Address)			

Hardware Type:

- 1 = Ethernet
- 2 = Experimental Ethernet
- 3 = Amateur Radio AX.25
- 4 = Proteon ProNET Token Ring
- 5 = Chaos
- 6 = IEEE 802 Networks, etc.

Protocol Type:

- IPv4 = 0x0800
- IPv6 = 0x86DD

Hardware Length:

- 6 for Ethernet

Protocol Length:

- 4 for IPv4

Operation Code:

- 1 For Request
- 2 For Reply

Notes: ____

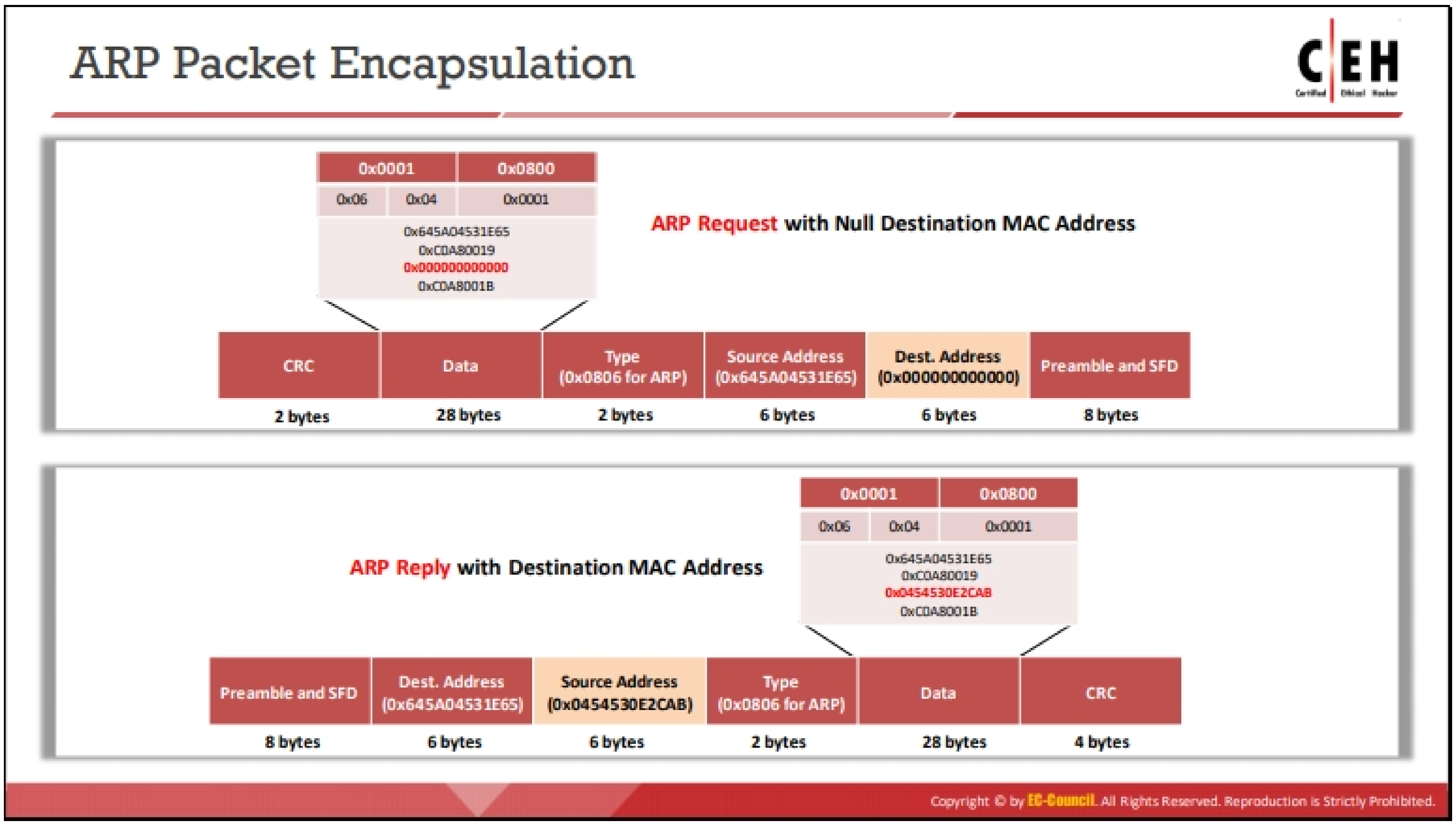
____

____

____

____

____



ARP Packet Encapsulation

ARP Request with Null Destination MAC Address

0x0001		0x0800
0x06	0x04	0x0001

0x645A04531E65
0xC0A80019
0x000000000000
0xC0A8001B

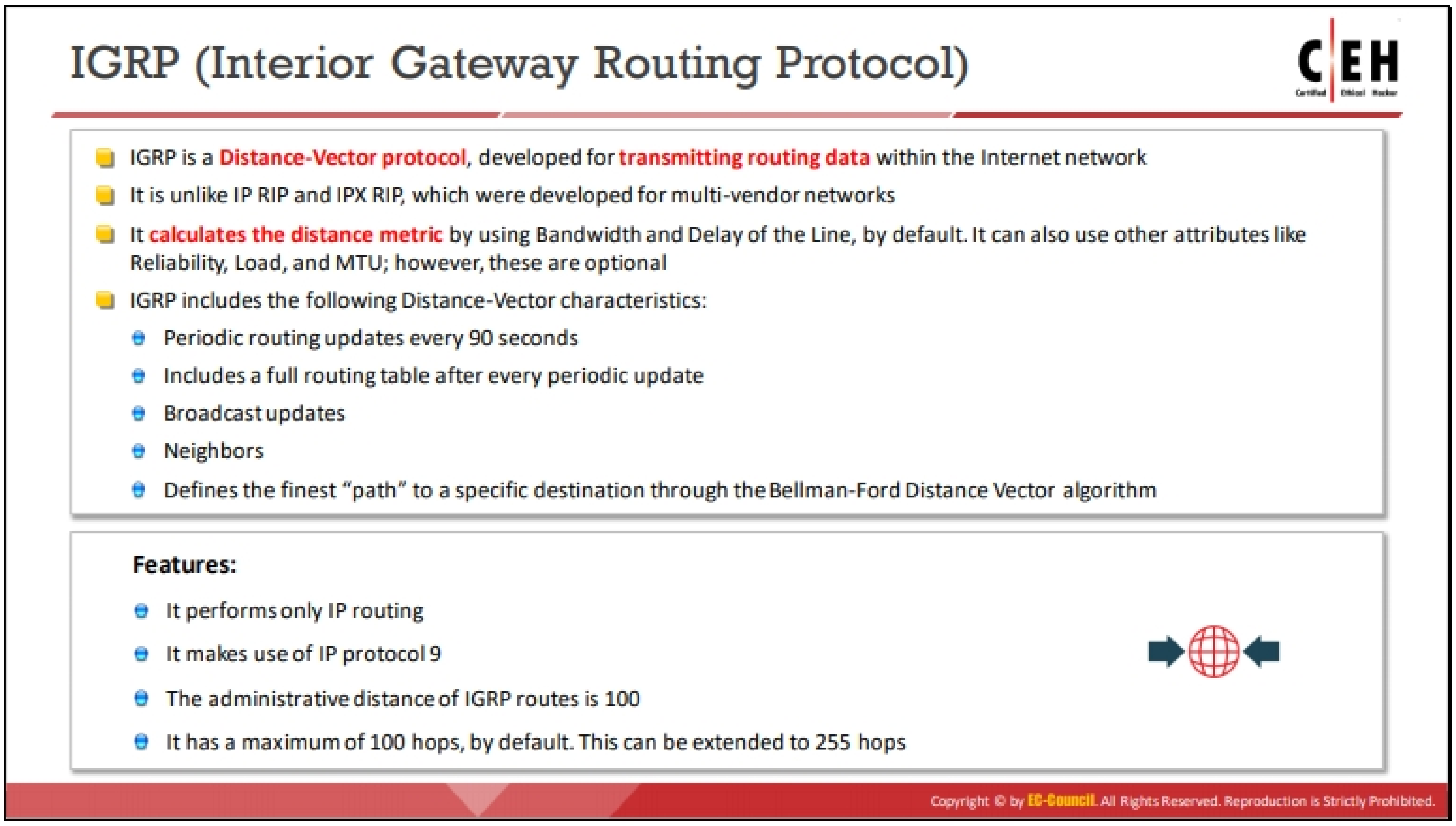
CRC	Data	Type (0x0806 for ARP)	Source Address (0x645A04531E65)	Dest. Address (0x000000000000)	Preamble and SFD
2 bytes	28 bytes	2 bytes	6 bytes	6 bytes	8 bytes

ARP Reply with Destination MAC Address

0x0001		0x0800
0x06	0x04	0x0001

0x645A04531E65
0xC0A80019
0x0454530E2CAB
0xC0A8001B

Preamble and SFD	Dest. Address (0x645A04531E65)	Source Address (0x0454530E2CAB)	Type (0x0806 for ARP)	Data	CRC
8 bytes	6 bytes	6 bytes	2 bytes	28 bytes	4 bytes



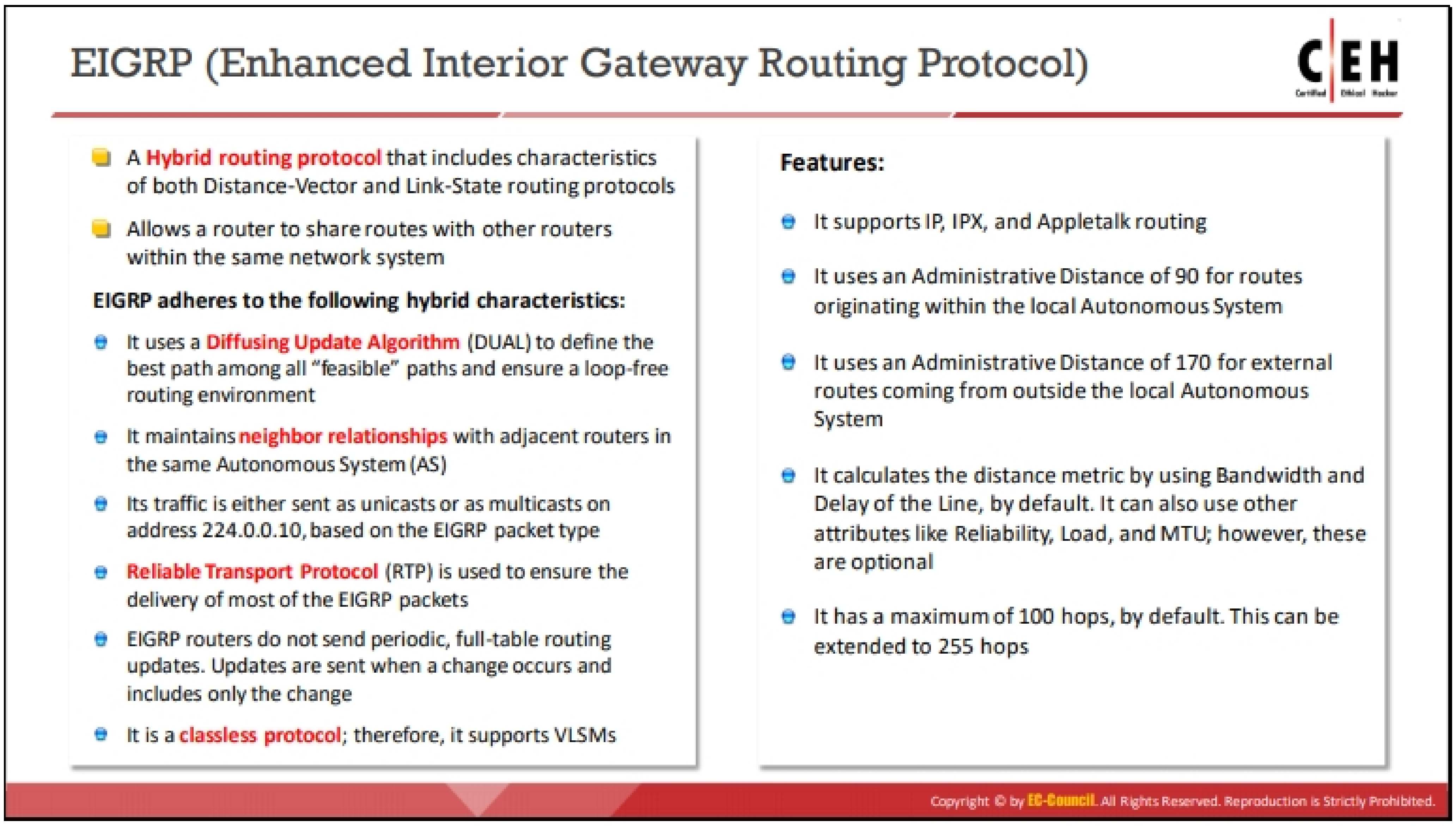
IGRP (Interior Gateway Routing Protocol)

- IGRP is a **Distance-Vector protocol**, developed for **transmitting routing data** within the Internet network
- It is unlike IP RIP and IPX RIP, which were developed for multi-vendor networks
- It **calculates the distance metric** by using Bandwidth and Delay of the Line, by default. It can also use other attributes like Reliability, Load, and MTU; however, these are optional
- IGRP includes the following Distance-Vector characteristics:
  - Periodic routing updates every 90 seconds
  - Includes a full routing table after every periodic update
  - Broadcast updates
  - Neighbors
  - Defines the finest "path" to a specific destination through the Bellman-Ford Distance Vector algorithm

Features:

- It performs only IP routing
- It makes use of IP protocol 9
- The administrative distance of IGRP routes is 100
- It has a maximum of 100 hops, by default. This can be extended to 255 hops

Notes:



EIGRP (Enhanced Interior Gateway Routing Protocol)

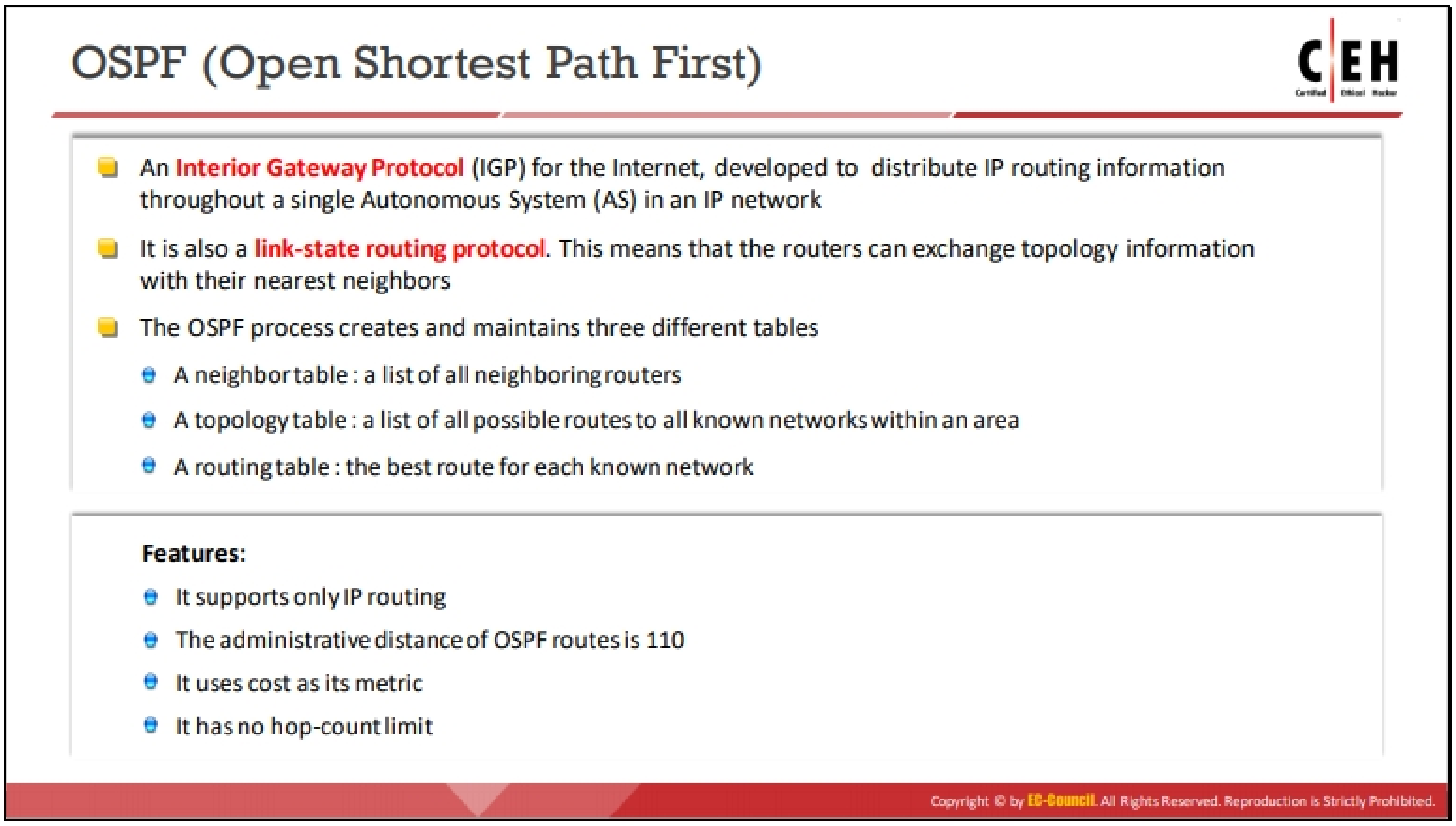
- A **Hybrid routing protocol** that includes characteristics of both Distance-Vector and Link-State routing protocols
- Allows a router to share routes with other routers within the same network system

EIGRP adheres to the following hybrid characteristics:

- It uses a **Diffusing Update Algorithm** (DUAL) to define the best path among all "feasible" paths and ensure a loop-free routing environment
- It maintains **neighbor relationships** with adjacent routers in the same Autonomous System (AS)
- Its traffic is either sent as unicasts or as multicasts on address 224.0.0.10, based on the EIGRP packet type
- **Reliable Transport Protocol** (RTP) is used to ensure the delivery of most of the EIGRP packets
- EIGRP routers do not send periodic, full-table routing updates. Updates are sent when a change occurs and includes only the change
- It is a **classless protocol**; therefore, it supports VLSMs

Features:

- It supports IP, IPX, and Appletalk routing
- It uses an Administrative Distance of 90 for routes originating within the local Autonomous System
- It uses an Administrative Distance of 170 for external routes coming from outside the local Autonomous System
- It calculates the distance metric by using Bandwidth and Delay of the Line, by default. It can also use other attributes like Reliability, Load, and MTU; however, these are optional
- It has a maximum of 100 hops, by default. This can be extended to 255 hops



OSPF (Open Shortest Path First)

- An **Interior Gateway Protocol** (IGP) for the Internet, developed to distribute IP routing information throughout a single Autonomous System (AS) in an IP network
- It is also a **link-state routing protocol**. This means that the routers can exchange topology information with their nearest neighbors
- The OSPF process creates and maintains three different tables
  - A neighbor table : a list of all neighboring routers
  - A topology table : a list of all possible routes to all known networks within an area
  - A routing table : the best route for each known network

Features:

- It supports only IP routing
- The administrative distance of OSPF routes is 110
- It uses cost as its metric
- It has no hop-count limit

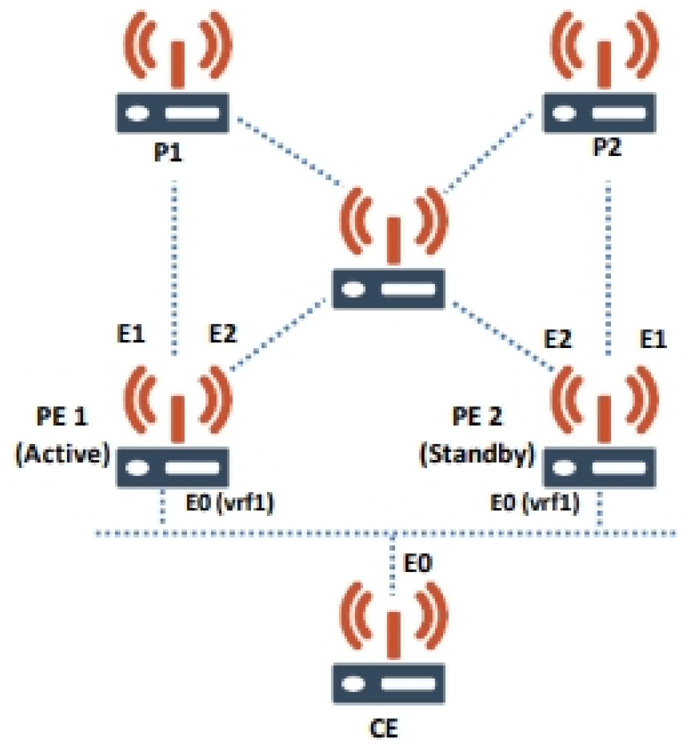
Notes:

HSRP (Hot Standby Router Protocol)

- A routing protocol used to establish a **fault-tolerant default gateway**. It allows the host computer to use multiple routers that act as a single virtual router
- A Cisco-developed redundancy protocol
- Virtual IP and MAC address are shared between the two routers
- To verify HSRP state, use the show standby command
- It makes sure that only the active router takes part in sending packets
- It is designed for multi access or broadcast LAN
- It gets automatically self updated when the MAC address is modified

Security issues:

- It can be vulnerable to DoS attacks



Virtual Router Redundancy Protocol (VRRP)

- VRRP is a computer networking protocol that provides for automatic assignment of available **Internet Protocol (IP) routers** to participating hosts

- It provides information on the **state of a router**. It does not provide information about routes processed or exchanged by the router

- If the physical router that is routing packets on behalf of the virtual router fails, another physical router is selected automatically to replace it

Security issues:

- It is vulnerable to DoS attacks

Notes:

BGP (Border Gateway Protocol)

- BGP is a routing protocol that **manages packets across the internet** through the exchange of information between host gateways or autonomous systems
- It makes routing decisions based on paths, reachability, hop counts, and network rules configured by the administrator
- Every BGP router **maintains a routing table** to forward the packet to the next hop
- BGP4 is the current version for internet routing. It helps Internet service providers (ISPs) to determine the routing of packets between each other

TCP/IP Protocol Suite

Link Layer Protocols

Notes: ____

____

____

____

____

____

Fiber Distributed Data Interface (FDDI)

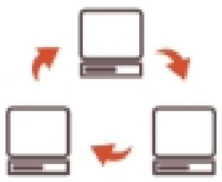
- FDDI-2 supports **voice** and **multimedia** communication to extensive geographical areas
- The optical standard for transferring data by means of **fiber optics** lines in a LAN up to 200 km
- Transfers data at the rate of **100 Mbps**

Comprised of two fiber optic rings

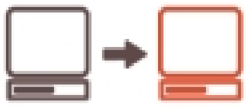
- **Primary ring:** Works in the network
- **Secondary ring:** Acts as backup and takes the position of primary ring in the case of network failure

Token Ring

- Local area network that connects multiple computers using a transmission link in either a **ring topology** or **star topology**



- Data flow is always **unidirectional**



Notes: ____

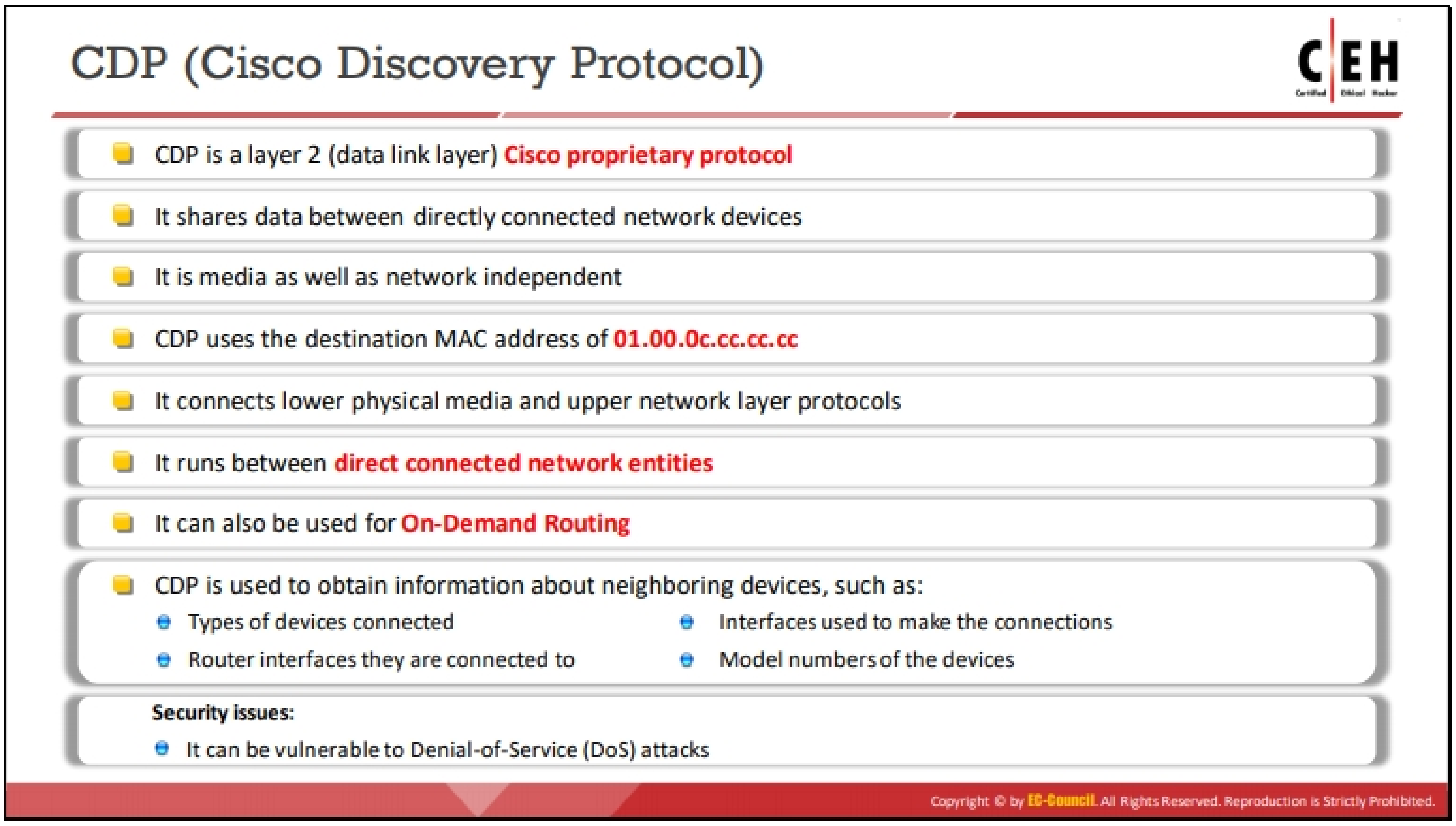
____

____

____

____

____

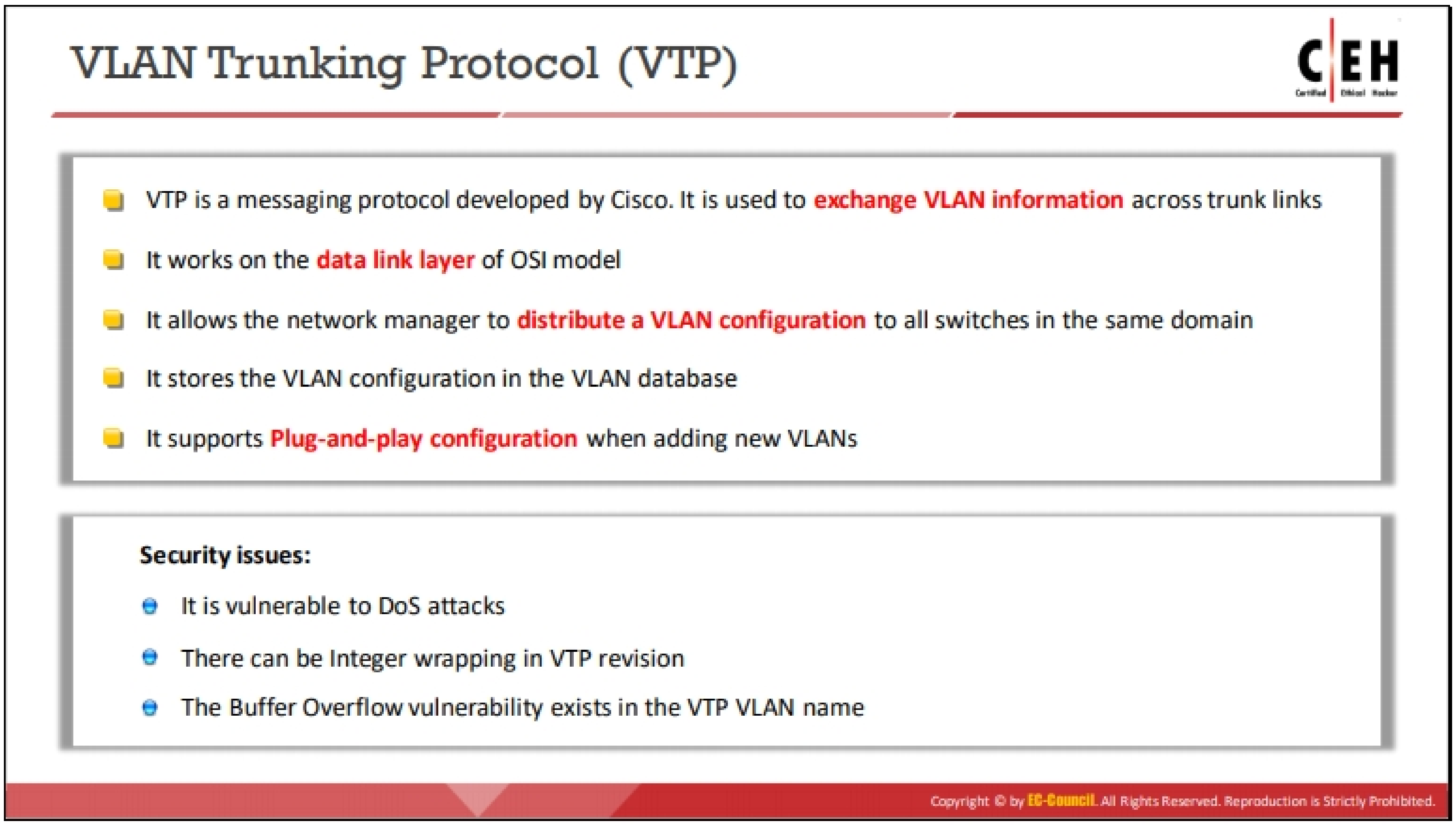


CDP (Cisco Discovery Protocol)

- CDP is a layer 2 (data link layer) **Cisco proprietary protocol**
- It shares data between directly connected network devices
- It is media as well as network independent
- CDP uses the destination MAC address of **01.00.0c.cc.cc.cc**
- It connects lower physical media and upper network layer protocols
- It runs between **direct connected network entities**
- It can also be used for **On-Demand Routing**
- CDP is used to obtain information about neighboring devices, such as:
  - Types of devices connected
  - Router interfaces they are connected to
  - Interfaces used to make the connections
  - Model numbers of the devices

Security issues:

- It can be vulnerable to Denial-of-Service (DoS) attacks



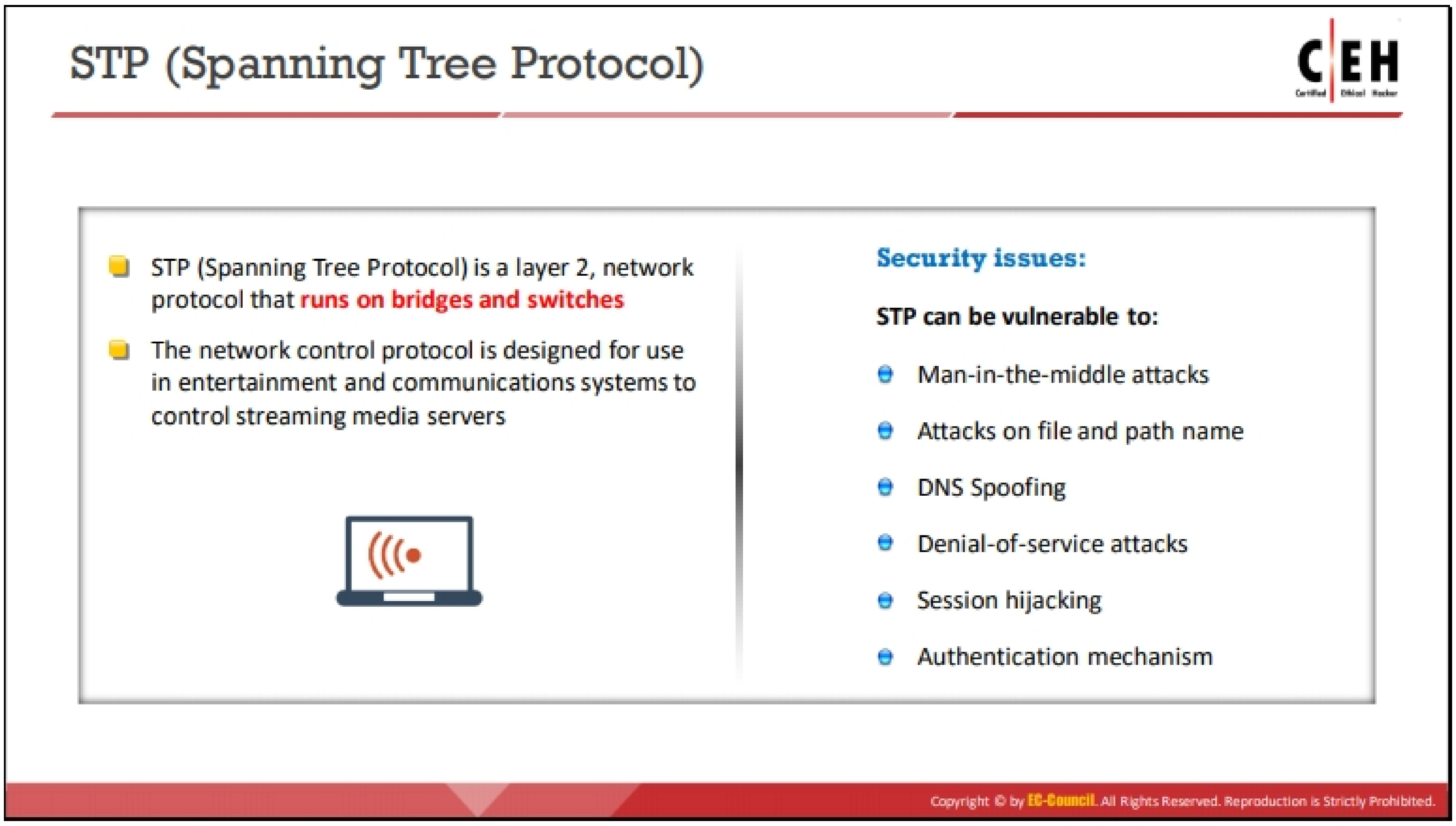
VLAN Trunking Protocol (VTP)

- VTP is a messaging protocol developed by Cisco. It is used to **exchange VLAN information** across trunk links
- It works on the **data link layer** of OSI model
- It allows the network manager to **distribute a VLAN configuration** to all switches in the same domain
- It stores the VLAN configuration in the VLAN database
- It supports **Plug-and-play configuration** when adding new VLANs

Security issues:

- It is vulnerable to DoS attacks
- There can be Integer wrapping in VTP revision
- The Buffer Overflow vulnerability exists in the VTP VLAN name

Notes: ____



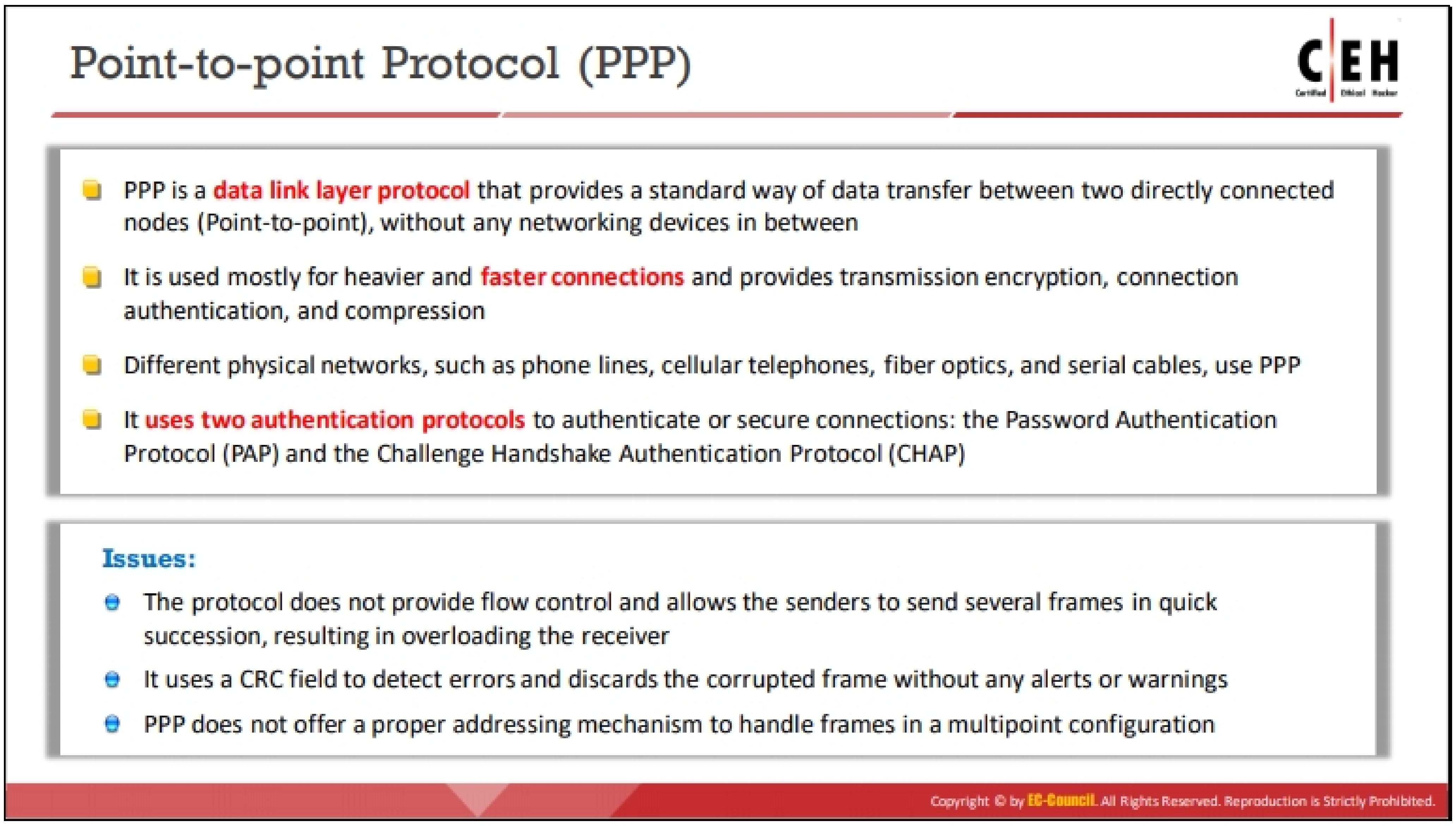
STP (Spanning Tree Protocol)

- STP (Spanning Tree Protocol) is a layer 2, network protocol that **runs on bridges and switches**
- The network control protocol is designed for use in entertainment and communications systems to control streaming media servers

Security issues:

STP can be vulnerable to:

- Man-in-the-middle attacks
- Attacks on file and path name
- DNS Spoofing
- Denial-of-service attacks
- Session hijacking
- Authentication mechanism



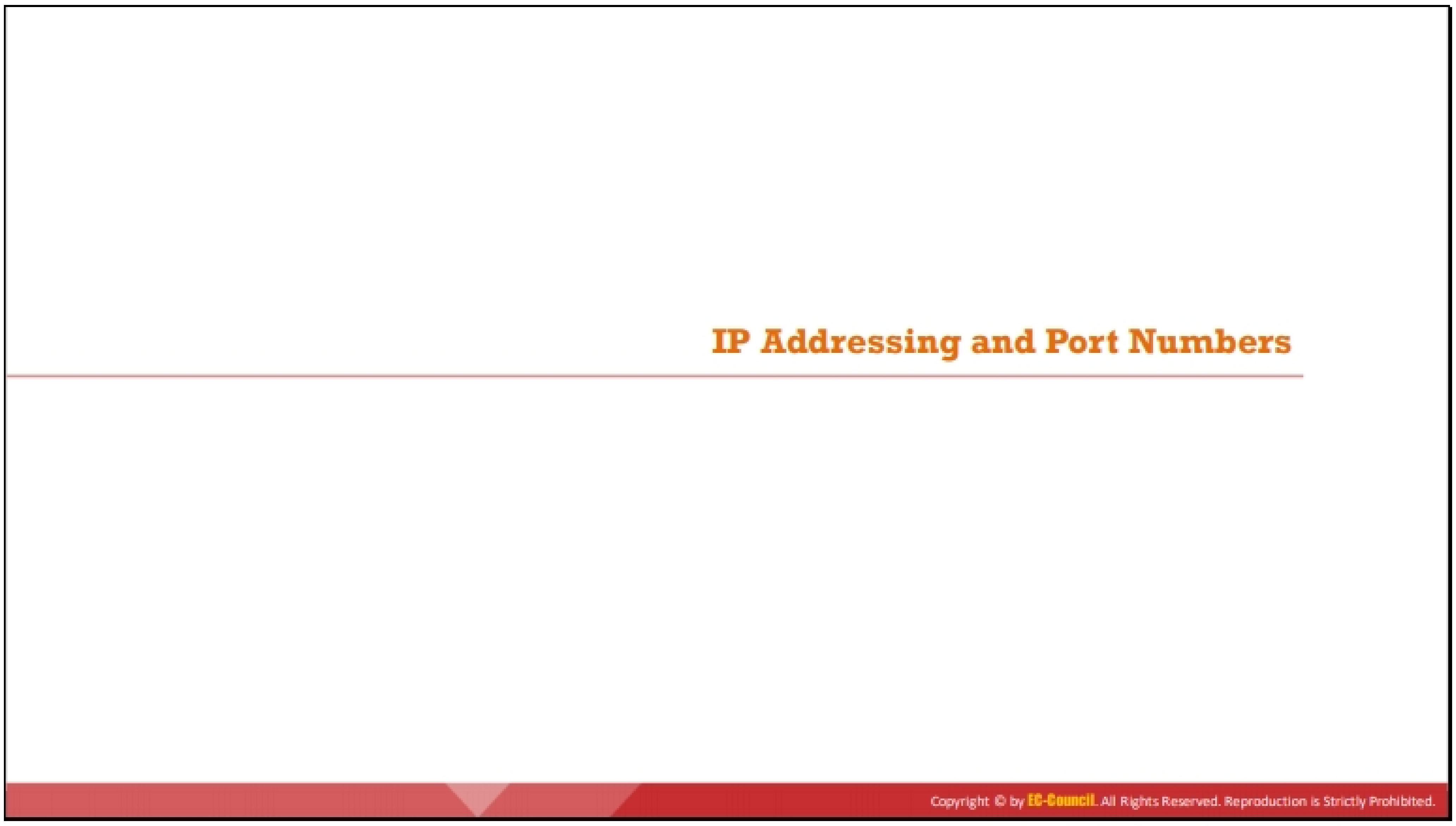
Point-to-point Protocol (PPP)

- PPP is a **data link layer protocol** that provides a standard way of data transfer between two directly connected nodes (Point-to-point), without any networking devices in between
- It is used mostly for heavier and **faster connections** and provides transmission encryption, connection authentication, and compression
- Different physical networks, such as phone lines, cellular telephones, fiber optics, and serial cables, use PPP
- It **uses two authentication protocols** to authenticate or secure connections: the Password Authentication Protocol (PAP) and the Challenge Handshake Authentication Protocol (CHAP)

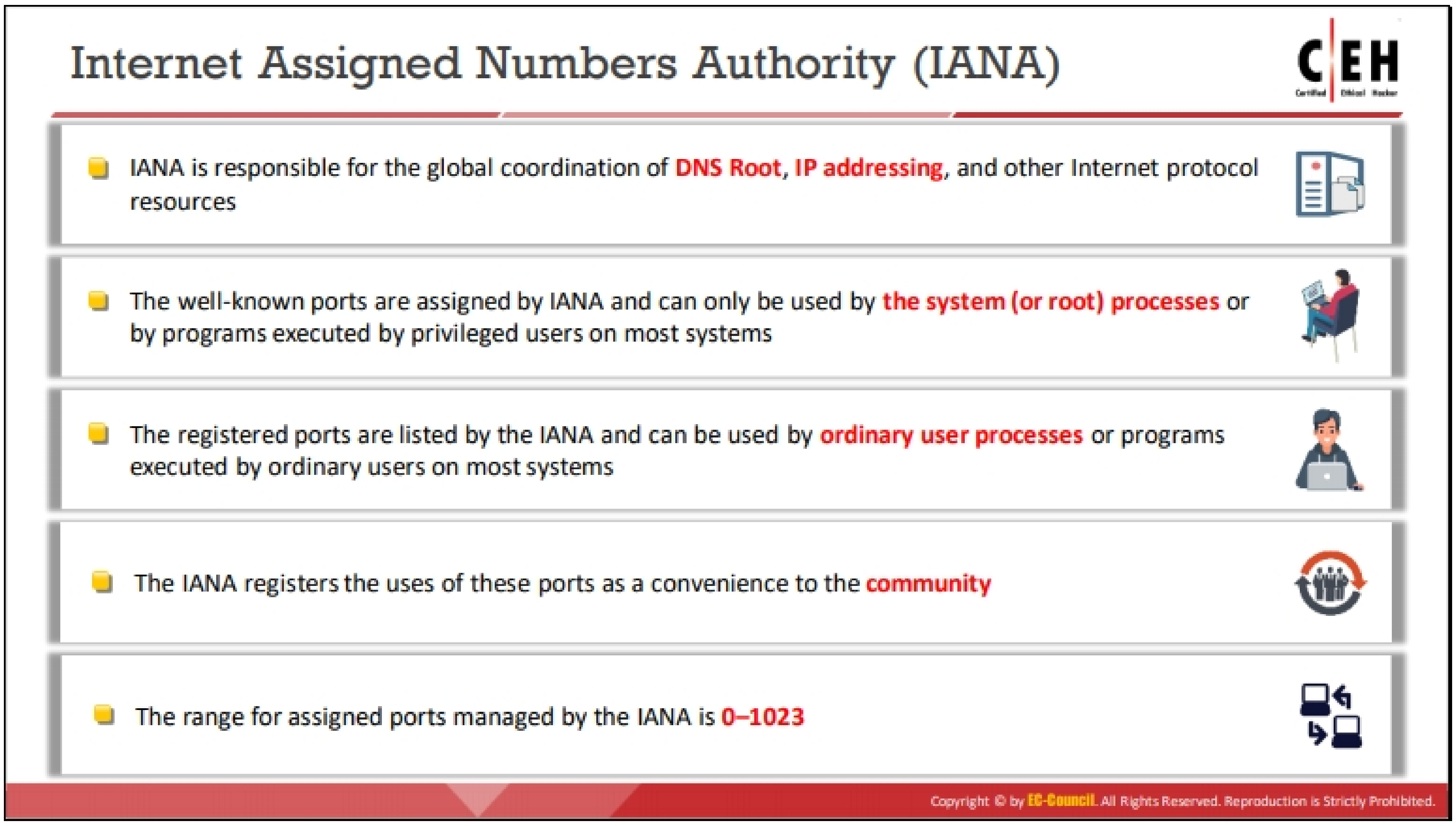
Issues:

- The protocol does not provide flow control and allows the senders to send several frames in quick succession, resulting in overloading the receiver
- It uses a CRC field to detect errors and discards the corrupted frame without any alerts or warnings
- PPP does not offer a proper addressing mechanism to handle frames in a multipoint configuration

Notes:



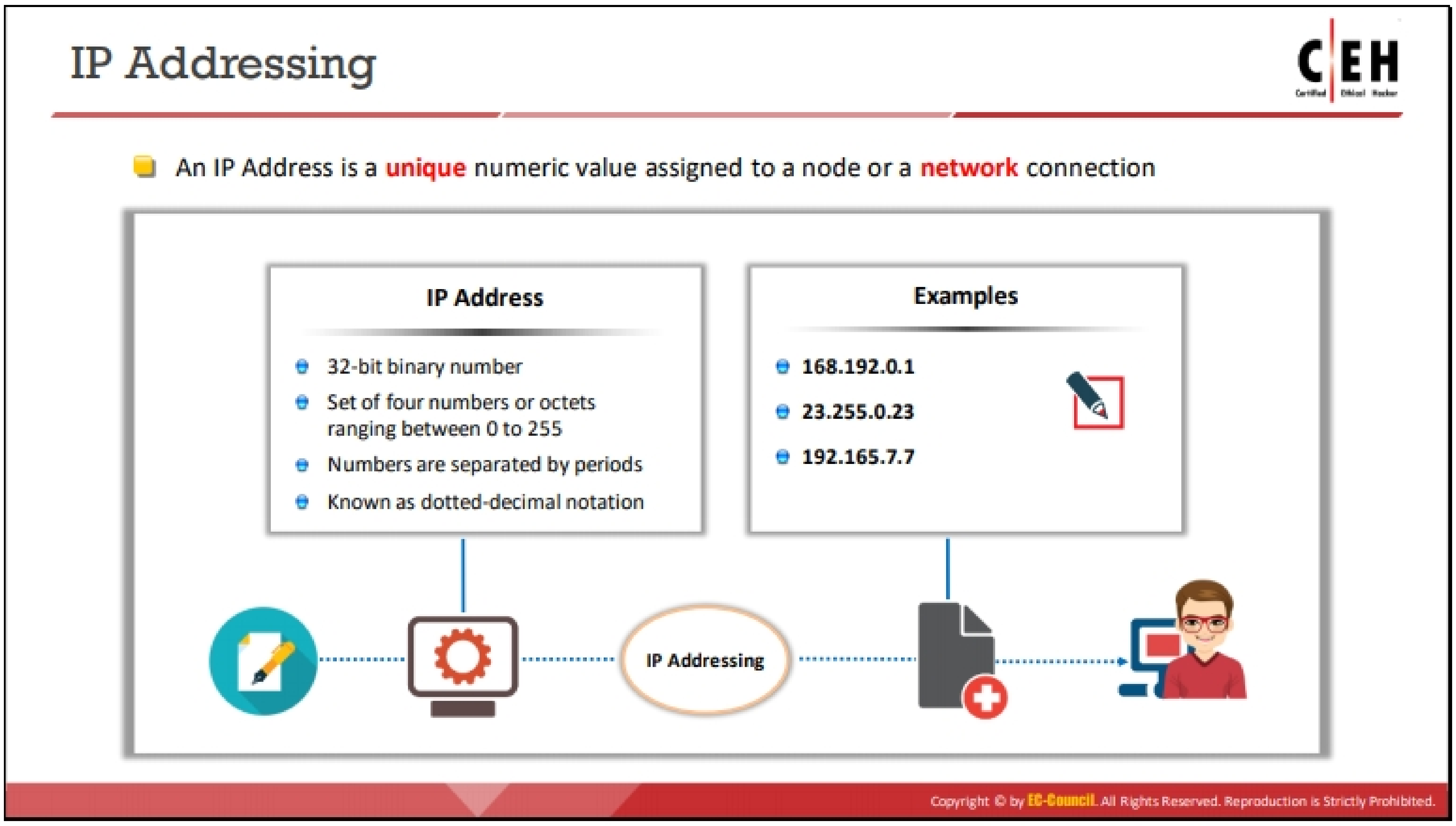
IP Addressing and Port Numbers



Internet Assigned Numbers Authority (IANA)

- IANA is responsible for the global coordination of **DNS Root**, **IP addressing**, and other Internet protocol resources
- The well-known ports are assigned by IANA and can only be used by **the system (or root) processes** or by programs executed by privileged users on most systems
- The registered ports are listed by the IANA and can be used by **ordinary user processes** or programs executed by ordinary users on most systems
- The IANA registers the uses of these ports as a convenience to the **community**
- The range for assigned ports managed by the IANA is **0–1023**

Notes: ____



IP Addressing

- An IP Address is a **unique** numeric value assigned to a node or a **network** connection

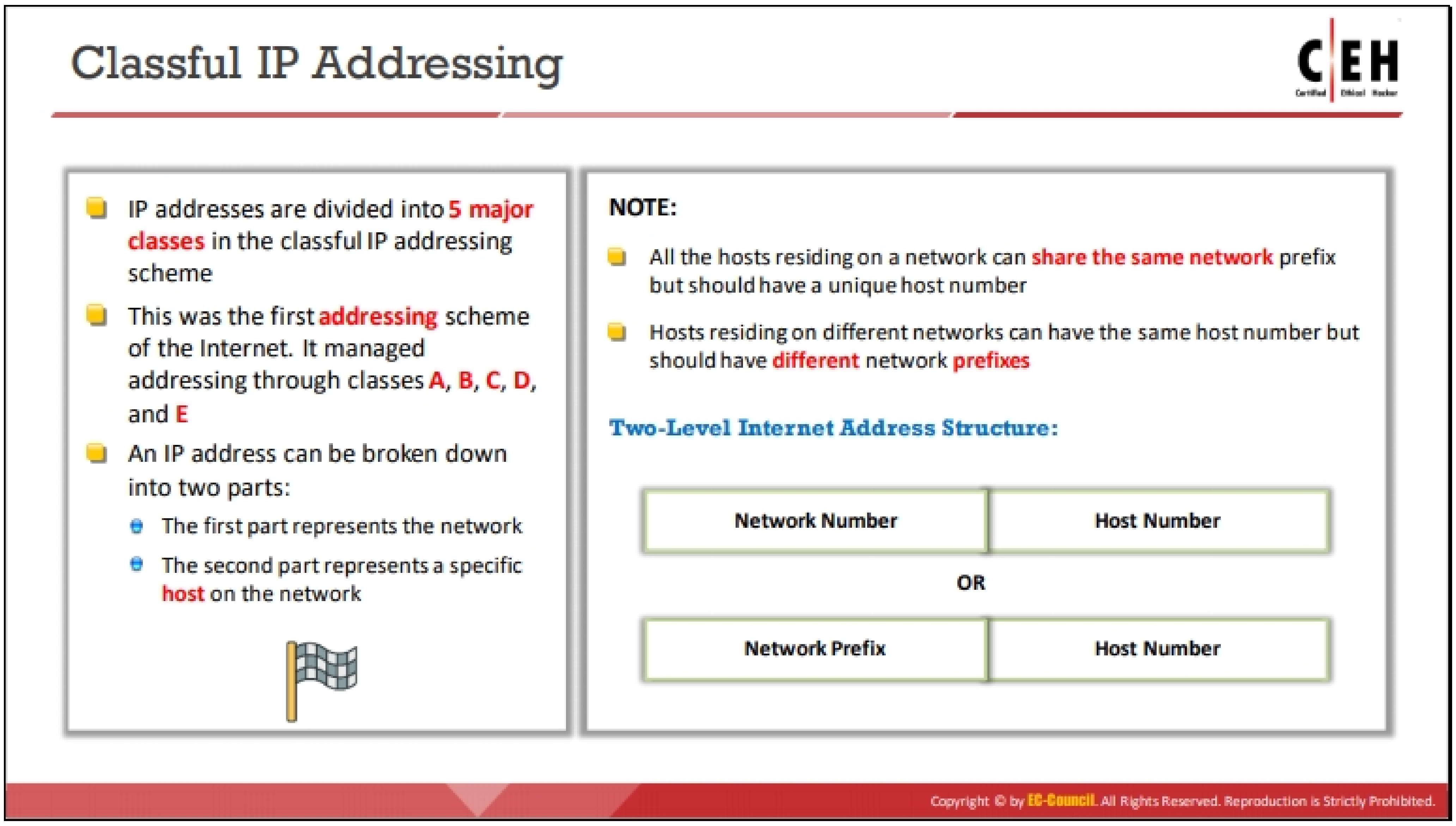
IP Address

- 32-bit binary number
- Set of four numbers or octets ranging between 0 to 255
- Numbers are separated by periods
- Known as dotted-decimal notation

Examples

- **168.192.0.1**
- **23.255.0.23**
- **192.165.7.7**

IP Addressing



Classful IP Addressing

- IP addresses are divided into **5 major classes** in the classful IP addressing scheme
- This was the first **addressing** scheme of the Internet. It managed addressing through classes **A**, **B**, **C**, **D**, and **E**
- An IP address can be broken down into two parts:
  - The first part represents the network
  - The second part represents a specific **host** on the network

NOTE:

- All the hosts residing on a network can **share the same network** prefix but should have a unique host number
- Hosts residing on different networks can have the same host number but should have **different** network **prefixes**

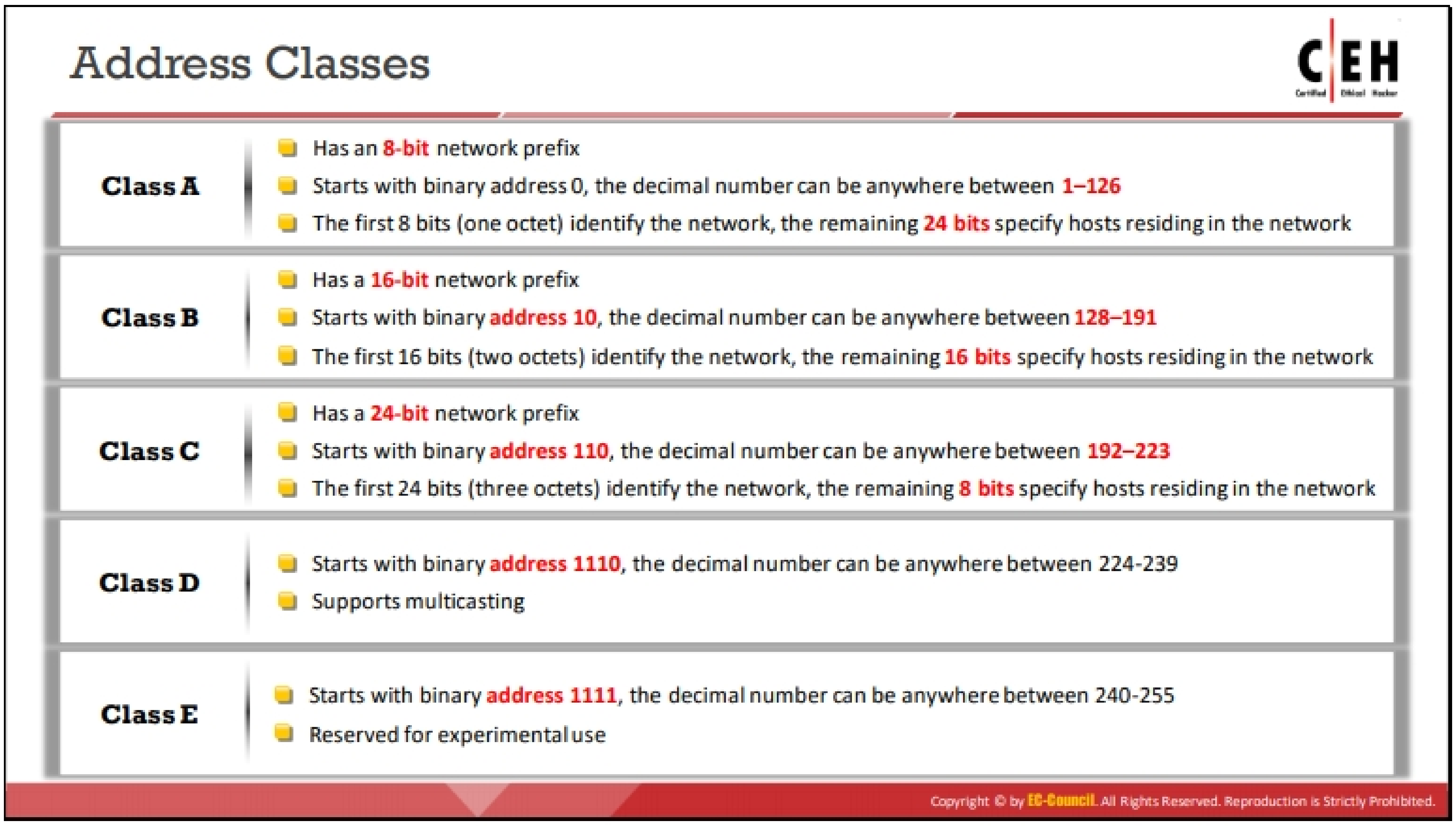
Two-Level Internet Address Structure:

Network Number	Host Number

OR

Network Prefix	Host Number

Notes: ____



Address Classes

Class A

- Has an **8-bit** network prefix
- Starts with binary address 0, the decimal number can be anywhere between **1–126**
- The first 8 bits (one octet) identify the network, the remaining **24 bits** specify hosts residing in the network

Class B

- Has a **16-bit** network prefix
- Starts with binary **address 10**, the decimal number can be anywhere between **128–191**
- The first 16 bits (two octets) identify the network, the remaining **16 bits** specify hosts residing in the network

Class C

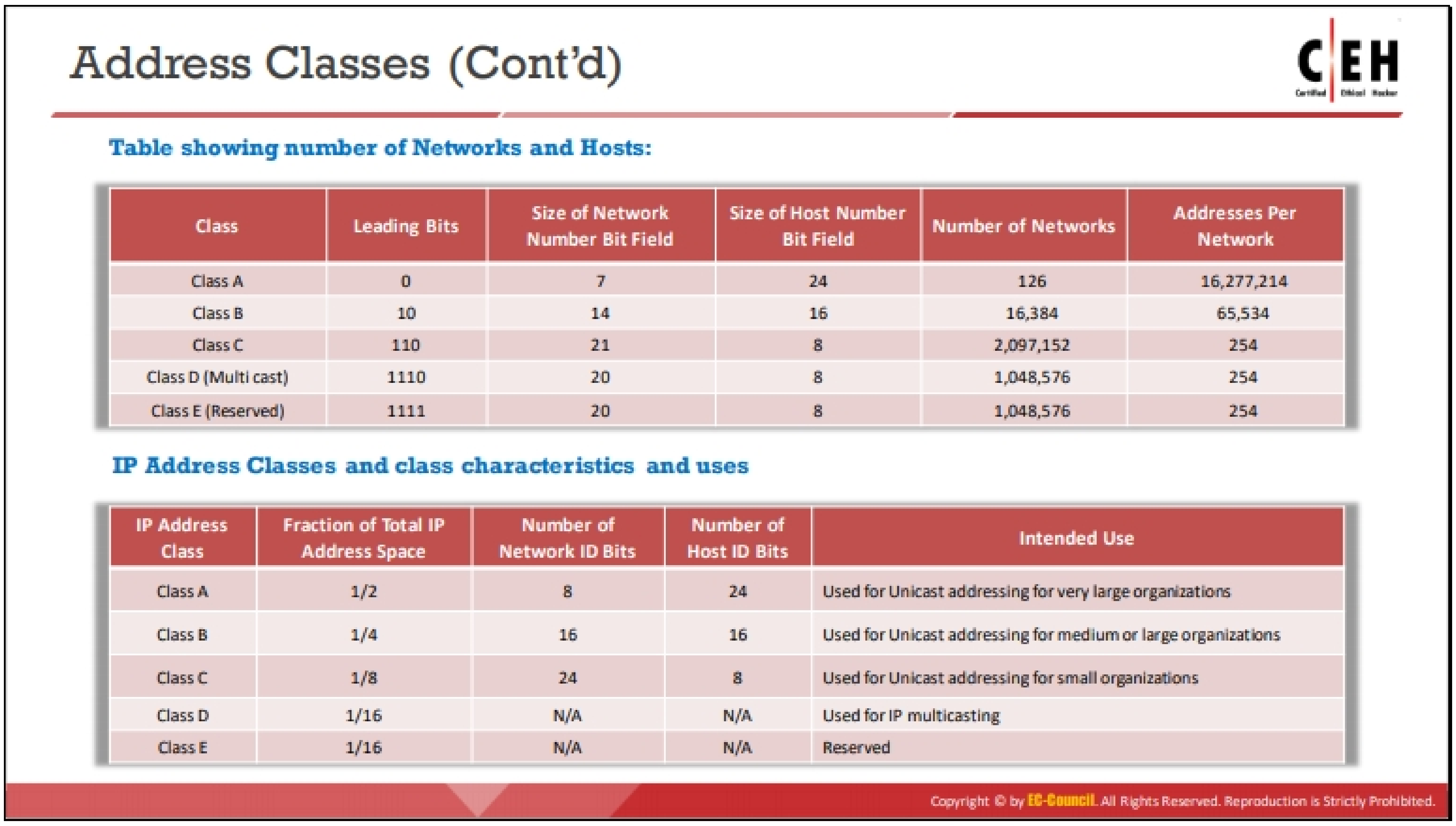
- Has a **24-bit** network prefix
- Starts with binary **address 110**, the decimal number can be anywhere between **192–223**
- The first 24 bits (three octets) identify the network, the remaining **8 bits** specify hosts residing in the network

Class D

- Starts with binary **address 1110**, the decimal number can be anywhere between 224-239
- Supports multicasting

Class E

- Starts with binary **address 1111**, the decimal number can be anywhere between 240-255
- Reserved for experimental use



Address Classes (Cont'd)

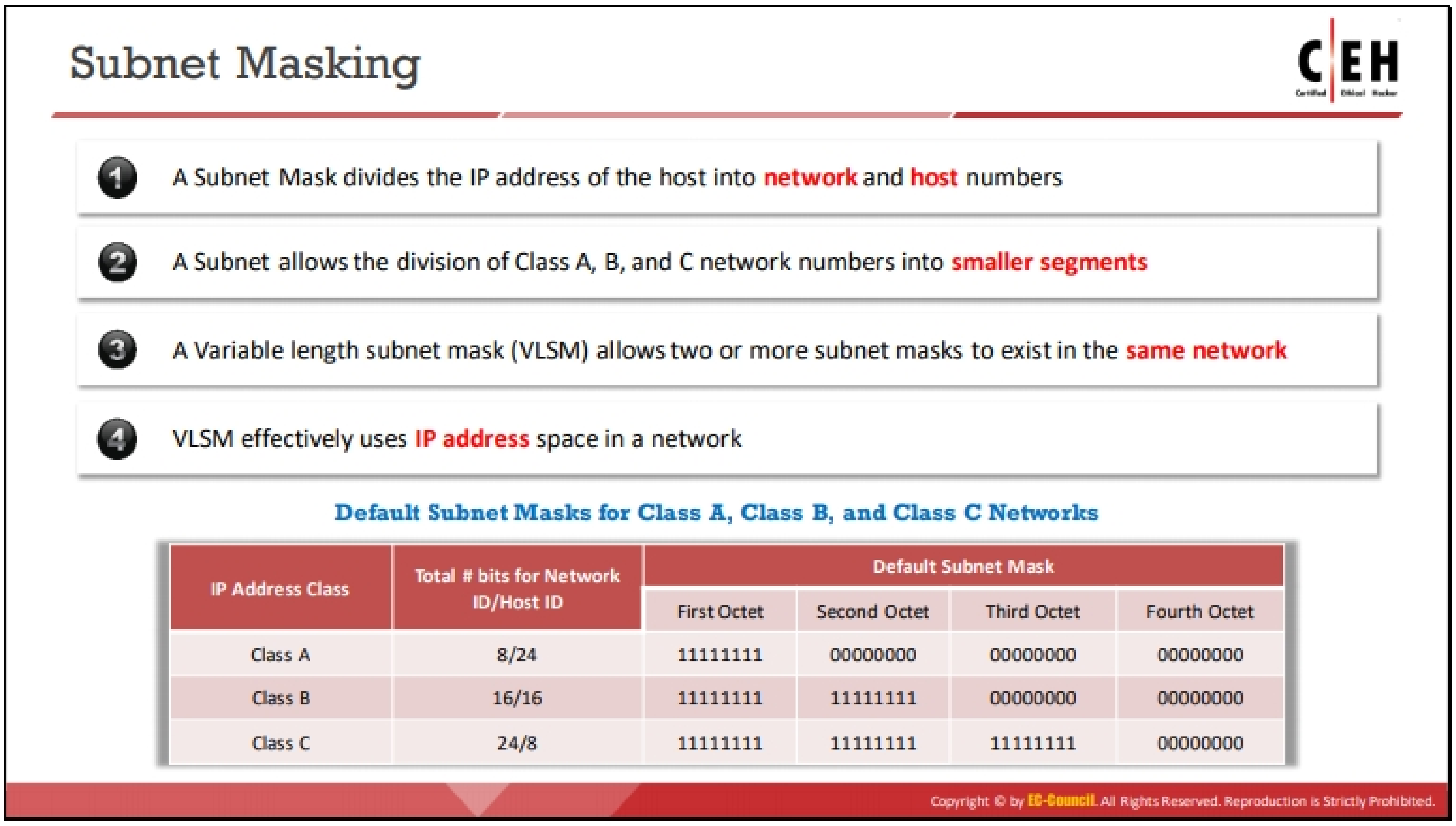
Table showing number of Networks and Hosts:

Class	Leading Bits	Size of Network Number Bit Field	Size of Host Number Bit Field	Number of Networks	Addresses Per Network
Class A	0	7	24	126	16,277,214
Class B	10	14	16	16,384	65,534
Class C	110	21	8	2,097,152	254
Class D (Multi cast)	1110	20	8	1,048,576	254
Class E (Reserved)	1111	20	8	1,048,576	254

IP Address Classes and class characteristics and uses

IP Address Class	Fraction of Total IP Address Space	Number of Network ID Bits	Number of Host ID Bits	Intended Use
Class A	1/2	8	24	Used for Unicast addressing for very large organizations
Class B	1/4	16	16	Used for Unicast addressing for medium or large organizations
Class C	1/8	24	8	Used for Unicast addressing for small organizations
Class D	1/16	N/A	N/A	Used for IP multicasting
Class E	1/16	N/A	N/A	Reserved

Notes: ____

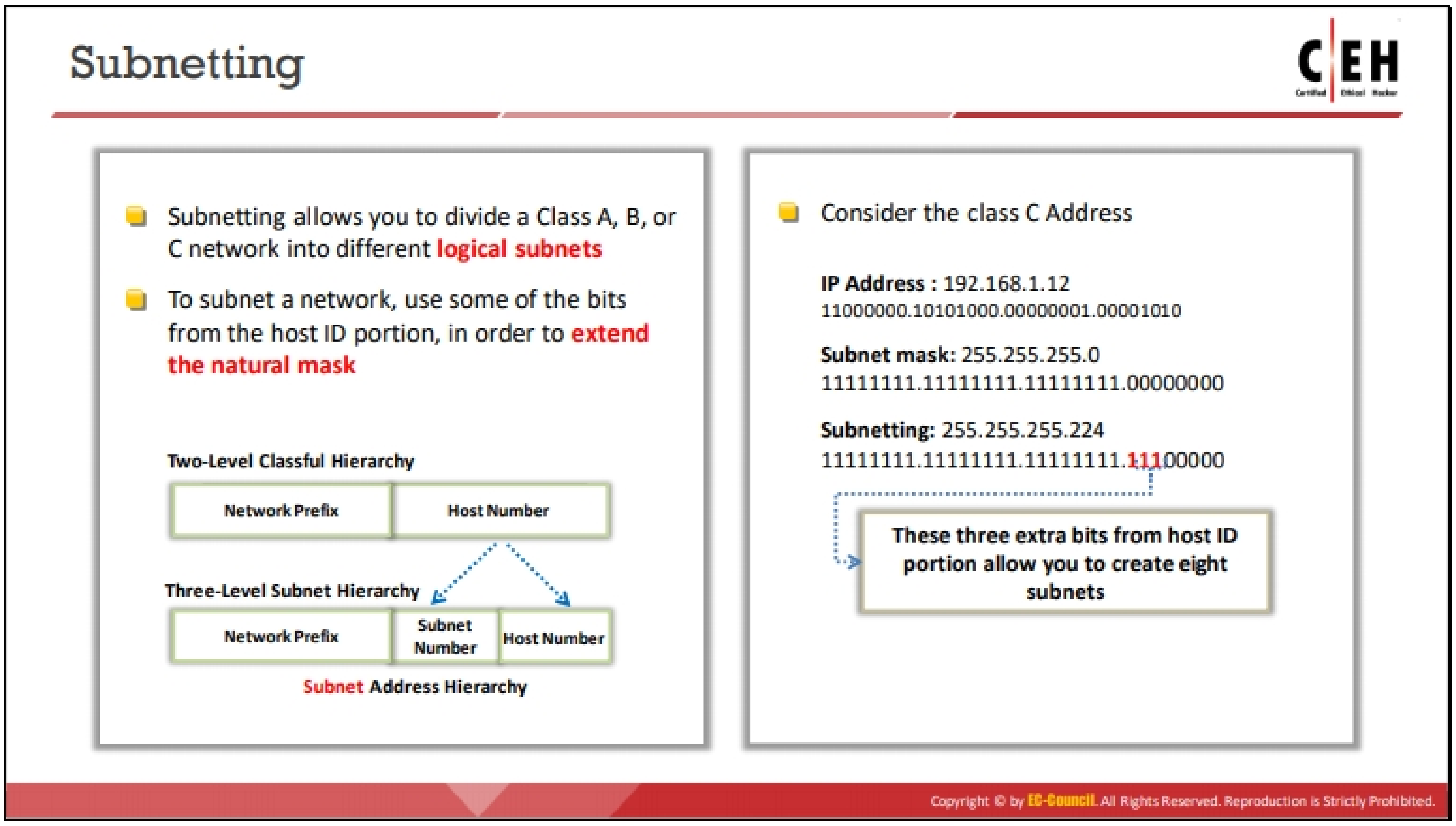


Subnet Masking

1. A Subnet Mask divides the IP address of the host into **network** and **host** numbers
2. A Subnet allows the division of Class A, B, and C network numbers into **smaller segments**
3. A Variable length subnet mask (VLSM) allows two or more subnet masks to exist in the **same network**
4. VLSM effectively uses **IP address** space in a network

Default Subnet Masks for Class A, Class B, and Class C Networks

IP Address Class	Total # bits for Network ID/Host ID	Default Subnet Mask			
		First Octet	Second Octet	Third Octet	Fourth Octet
Class A	8/24	11111111	00000000	00000000	00000000
Class B	16/16	11111111	11111111	00000000	00000000
Class C	24/8	11111111	11111111	11111111	00000000



Subnetting

- Subnetting allows you to divide a Class A, B, or C network into different **logical subnets**
- To subnet a network, use some of the bits from the host ID portion, in order to **extend the natural mask**

Two-Level Classful Hierarchy

Network Prefix	Host Number

Three-Level Subnet Hierarchy

Network Prefix	Subnet Number	Host Number

Subnet Address Hierarchy

- Consider the class C Address

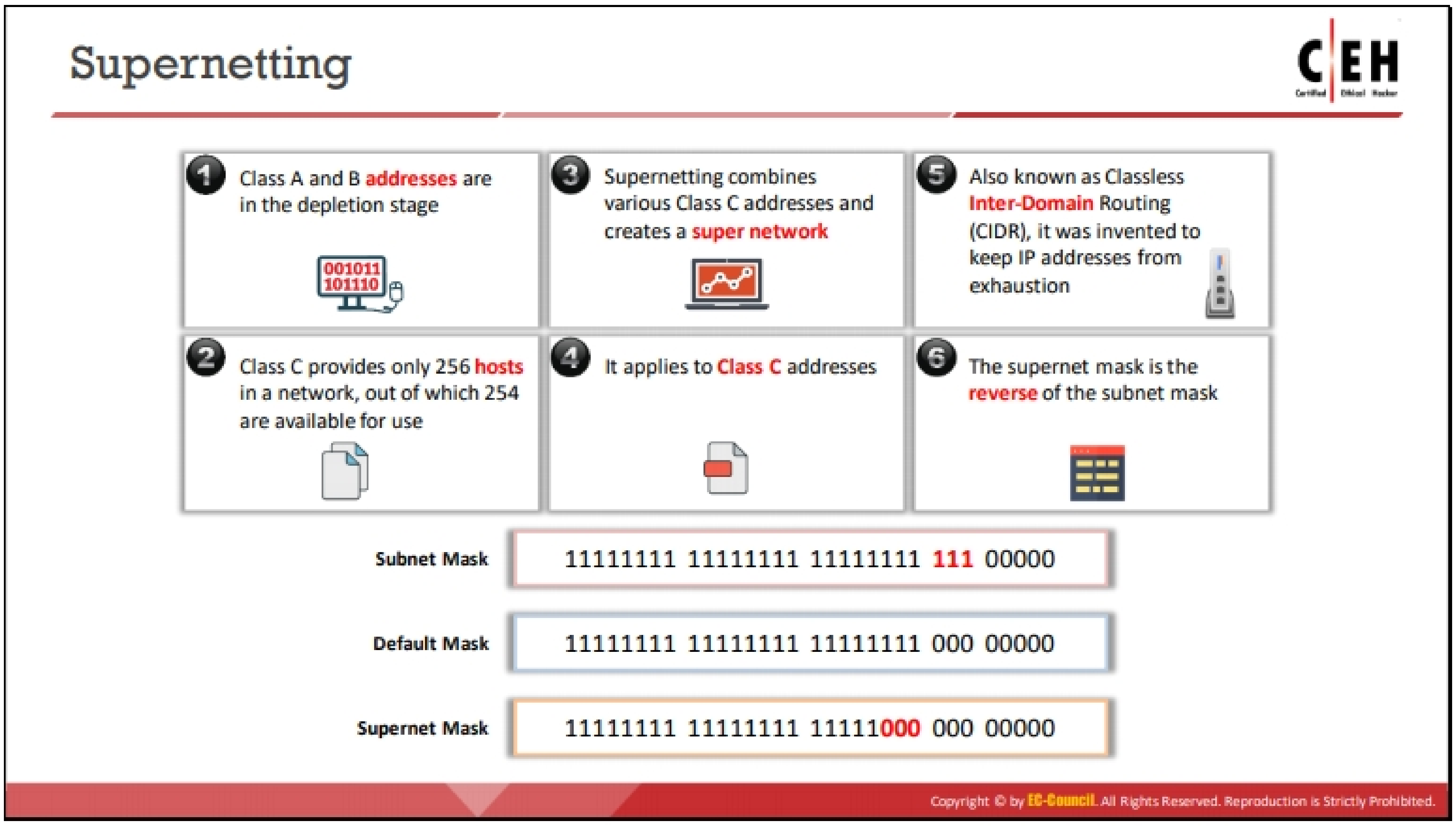
IP Address : 192.168.1.12
11000000.10101000.00000001.00001010

Subnet mask: 255.255.255.0
11111111.11111111.11111111.00000000

Subnetting: 255.255.255.224
11111111.11111111.11111111.11100000

These three extra bits from host ID portion allow you to create eight subnets

Notes:



Supernetting

① Class A and B addresses are in the depletion stage

② Class C provides only 256 hosts in a network, out of which 254 are available for use

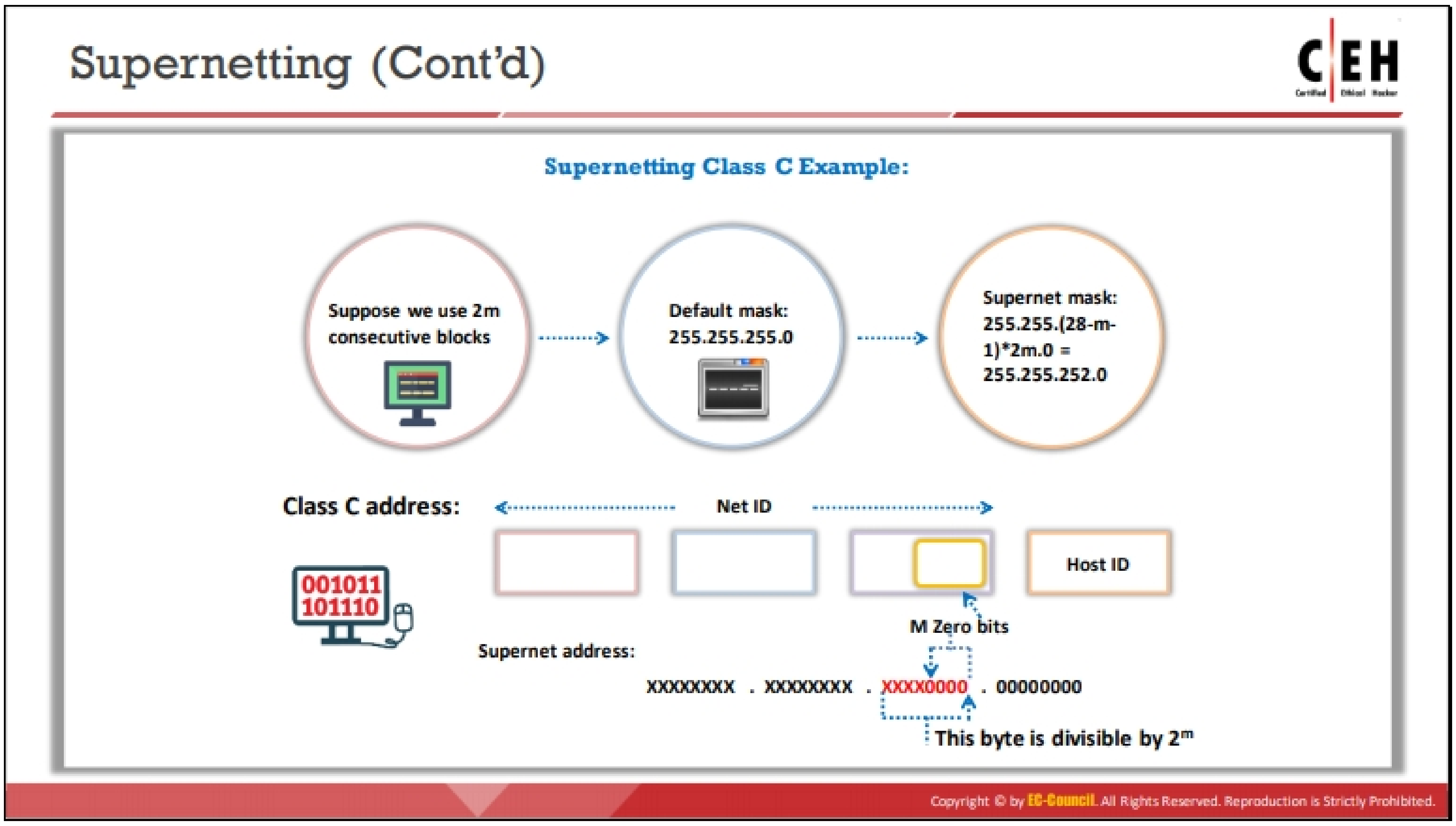
③ Supernetting combines various Class C addresses and creates a super network

④ It applies to Class C addresses

⑤ Also known as Classless Inter-Domain Routing (CIDR), it was invented to keep IP addresses from exhaustion

⑥ The supernet mask is the reverse of the subnet mask

Subnet Mask	11111111 11111111 11111111 111 00000
Default Mask	11111111 11111111 11111111 000 00000
Supernet Mask	11111111 11111111 11111000 000 00000



Supernetting (Cont'd)

Supernetting Class C Example:

Suppose we use 2m consecutive blocks

Default mask: 255.255.255.0

Supernet mask: 255.255.(28-m-1)*2m.0 = 255.255.252.0

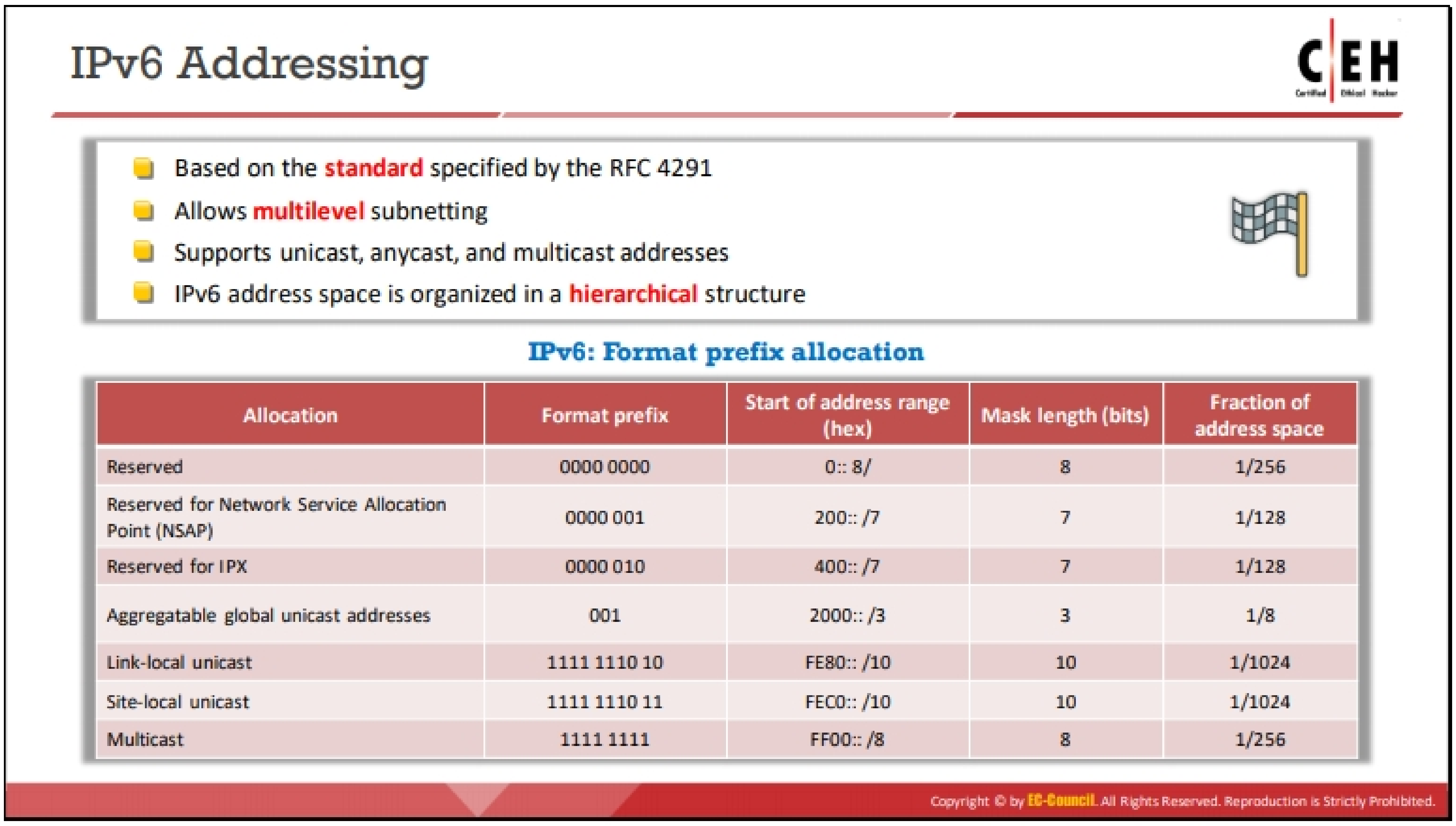
Class C address:

Supernet address:

XXXXXXXX . XXXXXXXX . XXXX0000 . 00000000

This byte is divisible by 2^m

Notes:

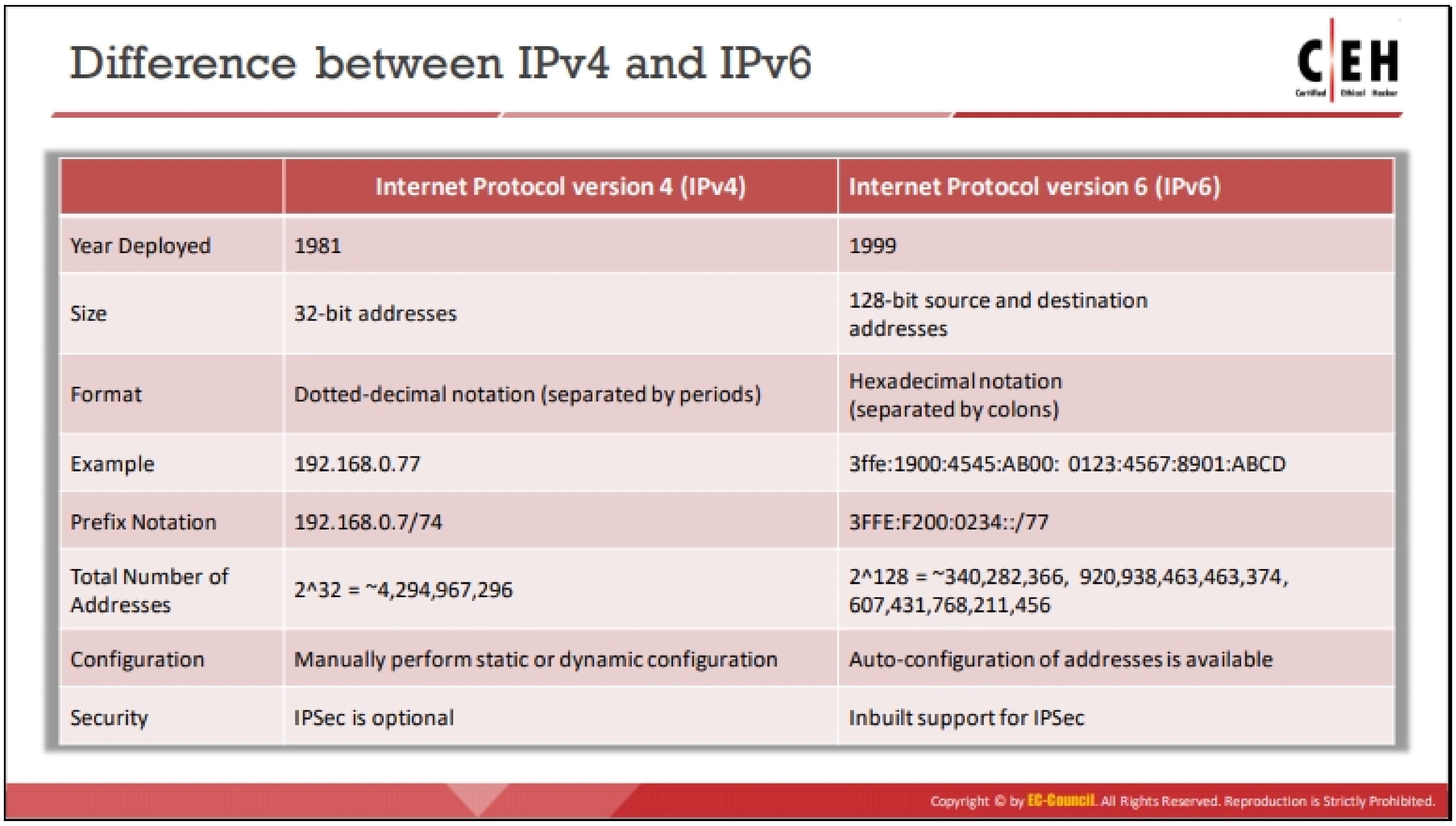


IPv6 Addressing

- Based on the **standard** specified by the RFC 4291
- Allows **multilevel** subnetting
- Supports unicast, anycast, and multicast addresses
- IPv6 address space is organized in a **hierarchical** structure

IPv6: Format prefix allocation

Allocation	Format prefix	Start of address range (hex)	Mask length (bits)	Fraction of address space
Reserved	0000 0000	0:: 8/	8	1/256
Reserved for Network Service Allocation Point (NSAP)	0000 001	200:: /7	7	1/128
Reserved for IPX	0000 010	400:: /7	7	1/128
Aggregatable global unicast addresses	001	2000:: /3	3	1/8
Link-local unicast	1111 1110 10	FE80:: /10	10	1/1024
Site-local unicast	1111 1110 11	FEC0:: /10	10	1/1024
Multicast	1111 1111	FF00:: /8	8	1/256



Difference between IPv4 and IPv6

	Internet Protocol version 4 (IPv4)	Internet Protocol version 6 (IPv6)
Year Deployed	1981	1999
Size	32-bit addresses	128-bit source and destination addresses
Format	Dotted-decimal notation (separated by periods)	Hexadecimal notation (separated by colons)
Example	192.168.0.77	3ffe:1900:4545:AB00: 0123:4567:8901:ABCD
Prefix Notation	192.168.0.7/74	3FFE:F200:0234::/77
Total Number of Addresses	2^32 = ~4,294,967,296	2^128 = ~340,282,366, 920,938,463,463,374, 607,431,768,211,456
Configuration	Manually perform static or dynamic configuration	Auto-configuration of addresses is available
Security	IPSec is optional	Inbuilt support for IPSec

Notes: ____

____

____

____

____

____

Port Numbers

- Both **TCP** and **UDP** use port (socket) numbers to pass information to the upper layers
- Port numbers are used to keep track of different **conversations** crossing the **network** simultaneously
- Conversations that do not involve an application with a well-known port number are **assigned port numbers** that are randomly selected from within a **specific range**
- Some ports are reserved in both **TCP** and **UDP**, although **applications** might not be written to support them
- End systems use **port numbers** to select the correct application for handling the **communication**

- Port numbers have the following assigned ranges:
  - Numbers below 1024 are considered well-known port numbers
  - Numbers above 1024 are dynamically assigned port numbers
  - Registered port numbers are those registered for vendor-specific applications; most of these are above 1024

Network Terminology

Notes: ____

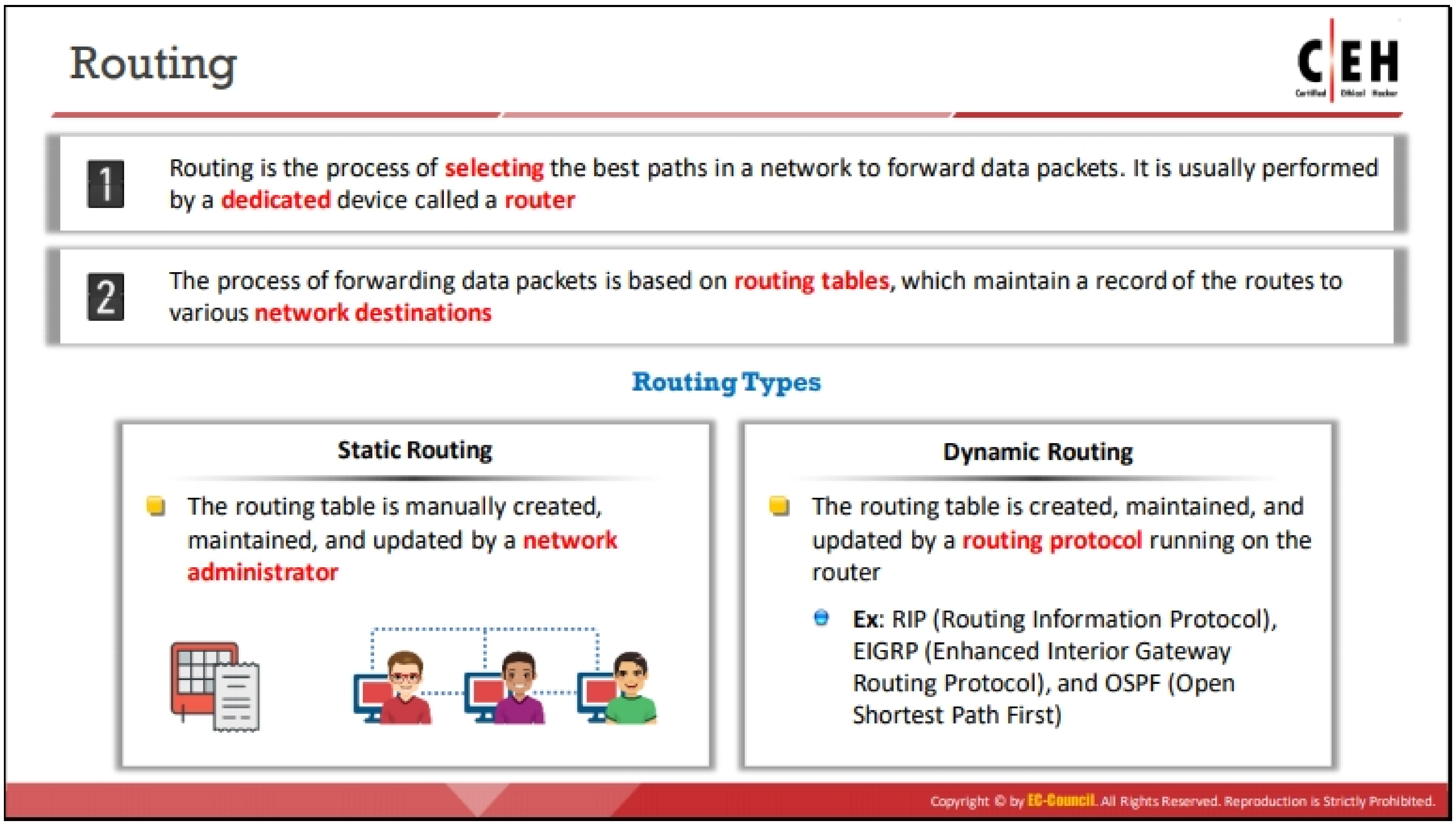
____

____

____

____

____



Routing

1. Routing is the process of **selecting** the best paths in a network to forward data packets. It is usually performed by a **dedicated** device called a **router**

2. The process of forwarding data packets is based on **routing tables**, which maintain a record of the routes to various **network destinations**

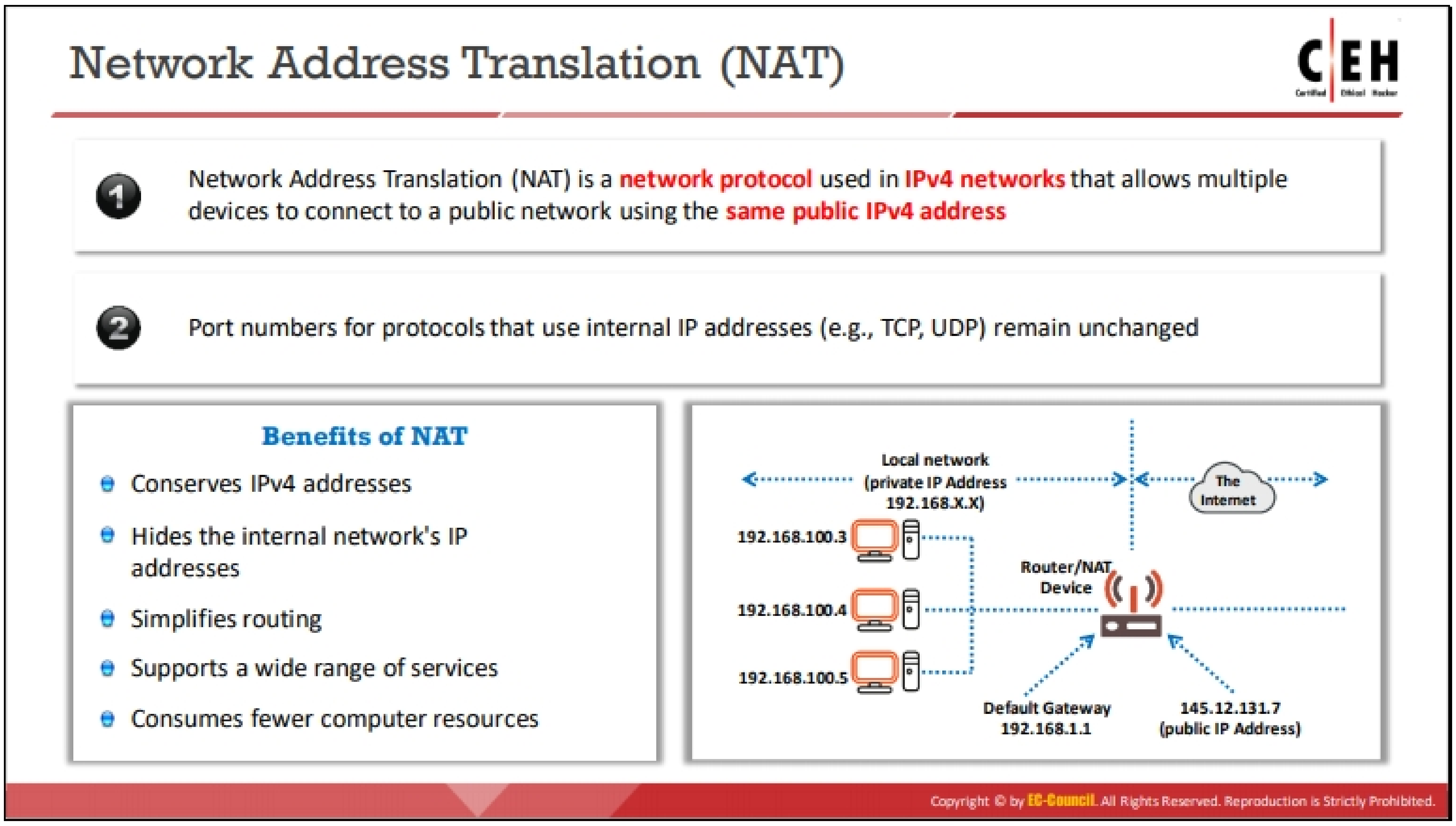
Routing Types

Static Routing

- The routing table is manually created, maintained, and updated by a **network administrator**

Dynamic Routing

- The routing table is created, maintained, and updated by a **routing protocol** running on the router
  - **Ex**: RIP (Routing Information Protocol), EIGRP (Enhanced Interior Gateway Routing Protocol), and OSPF (Open Shortest Path First)



Network Address Translation (NAT)

❶ Network Address Translation (NAT) is a **network protocol** used in **IPv4 networks** that allows multiple devices to connect to a public network using the **same public IPv4 address**

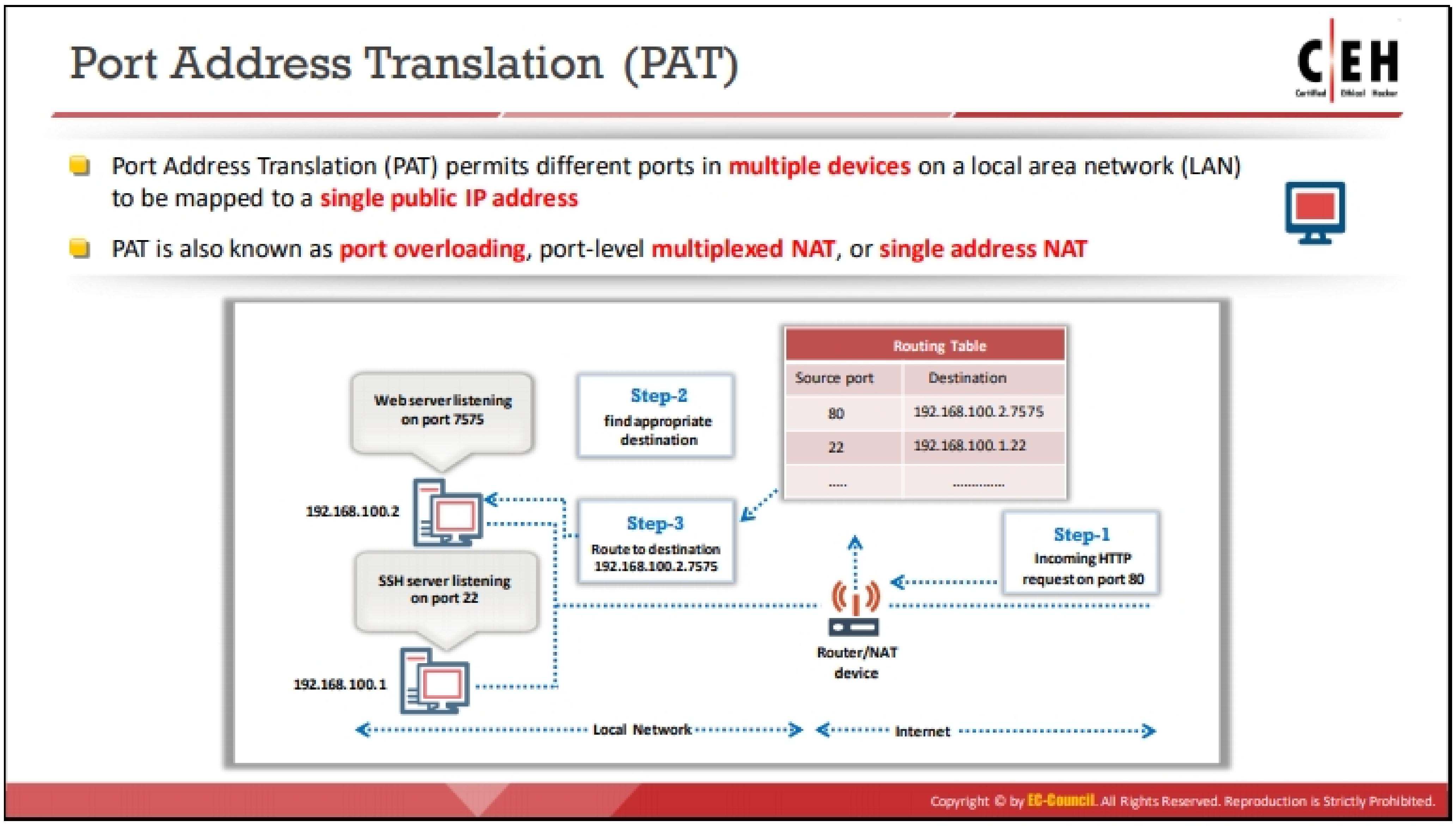
❷ Port numbers for protocols that use internal IP addresses (e.g., TCP, UDP) remain unchanged

Benefits of NAT

- Conserves IPv4 addresses
- Hides the internal network's IP addresses
- Simplifies routing
- Supports a wide range of services
- Consumes fewer computer resources

Local network
(private IP Address
192.168.X.X)
The Internet
192.168.100.3
192.168.100.4
192.168.100.5
Router/NAT Device
Default Gateway
192.168.1.1
145.12.131.7
(public IP Address)

Notes: ____

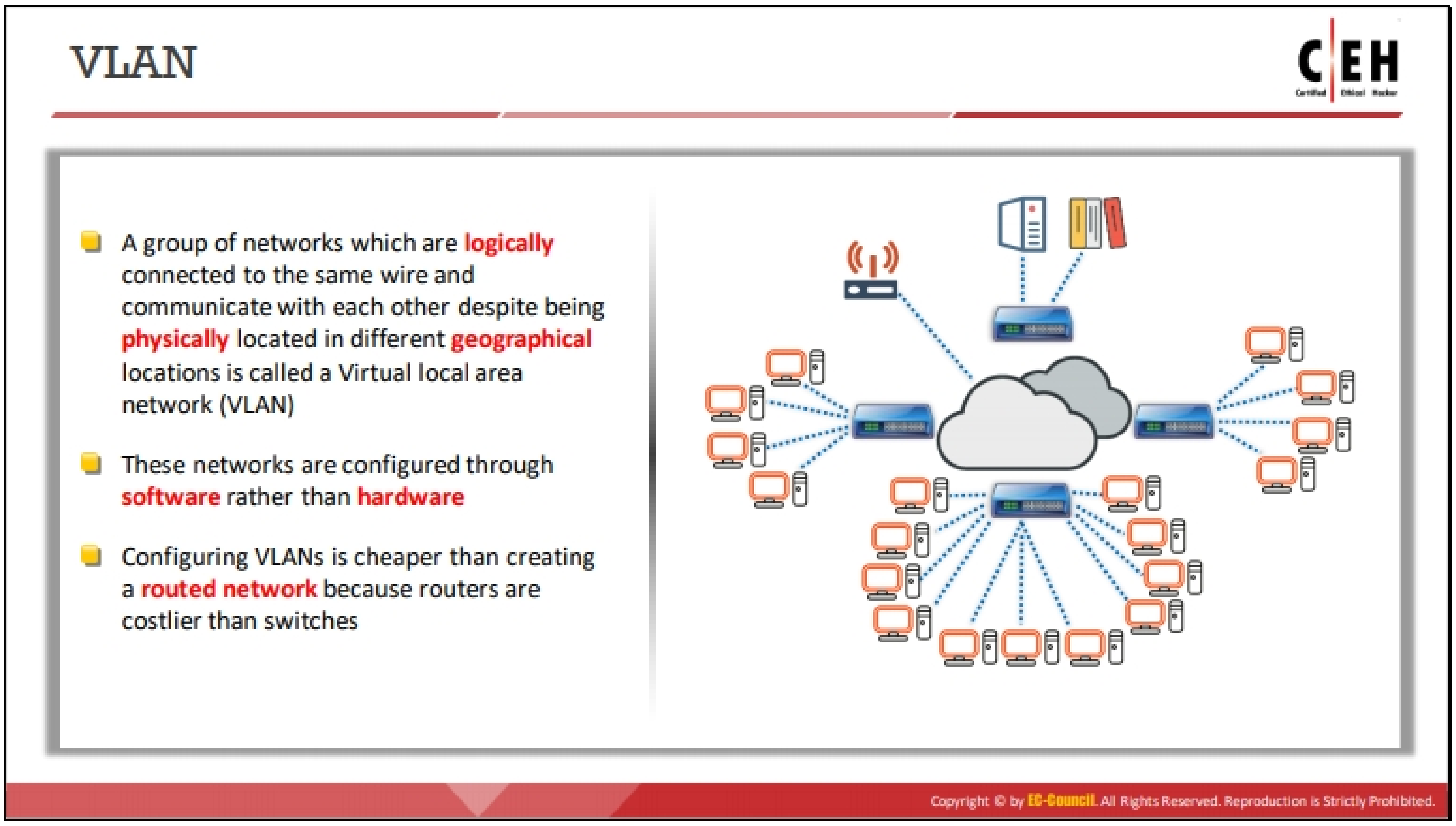


Port Address Translation (PAT)

- Port Address Translation (PAT) permits different ports in **multiple devices** on a local area network (LAN) to be mapped to a **single public IP address**
- PAT is also known as **port overloading**, port-level **multiplexed NAT**, or **single address NAT**

Web server listening on port 7575
192.168.100.2
SSH server listening on port 22
192.168.100.1
Step-2
find appropriate destination
Step-3
Route to destination 192.168.100.2.7575
Step-1
Incoming HTTP request on port 80
Router/NAT device
Local Network
Internet

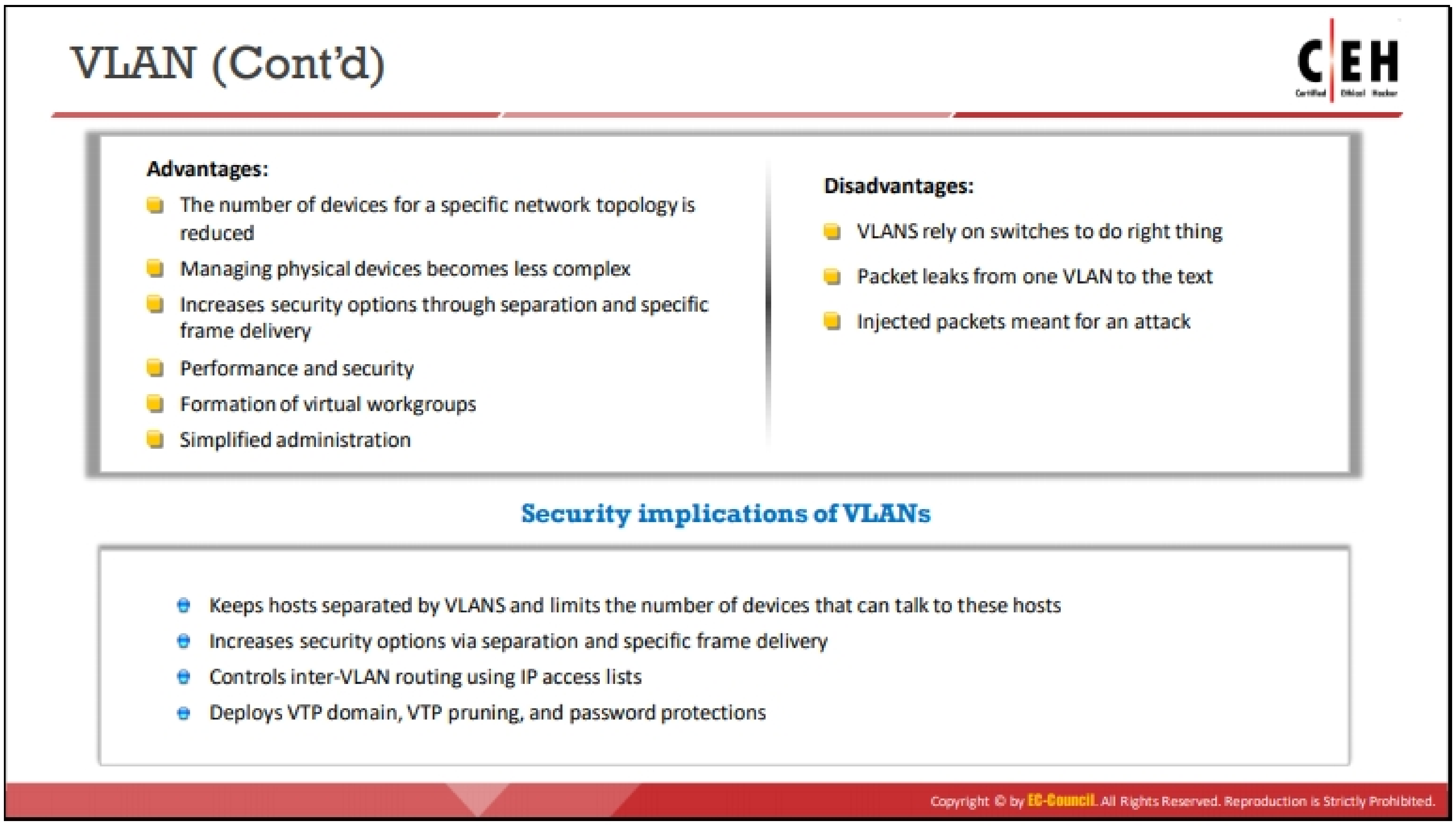
Routing Table	
Source port	Destination
80	192.168.100.2.7575
22	192.168.100.1.22
.....	....



VLAN

- A group of networks which are **logically** connected to the same wire and communicate with each other despite being **physically** located in different **geographical** locations is called a Virtual local area network (VLAN)
- These networks are configured through **software** rather than **hardware**
- Configuring VLANs is cheaper than creating a **routed network** because routers are costlier than switches

Notes: ______________________________



VLAN (Cont'd)

Advantages:

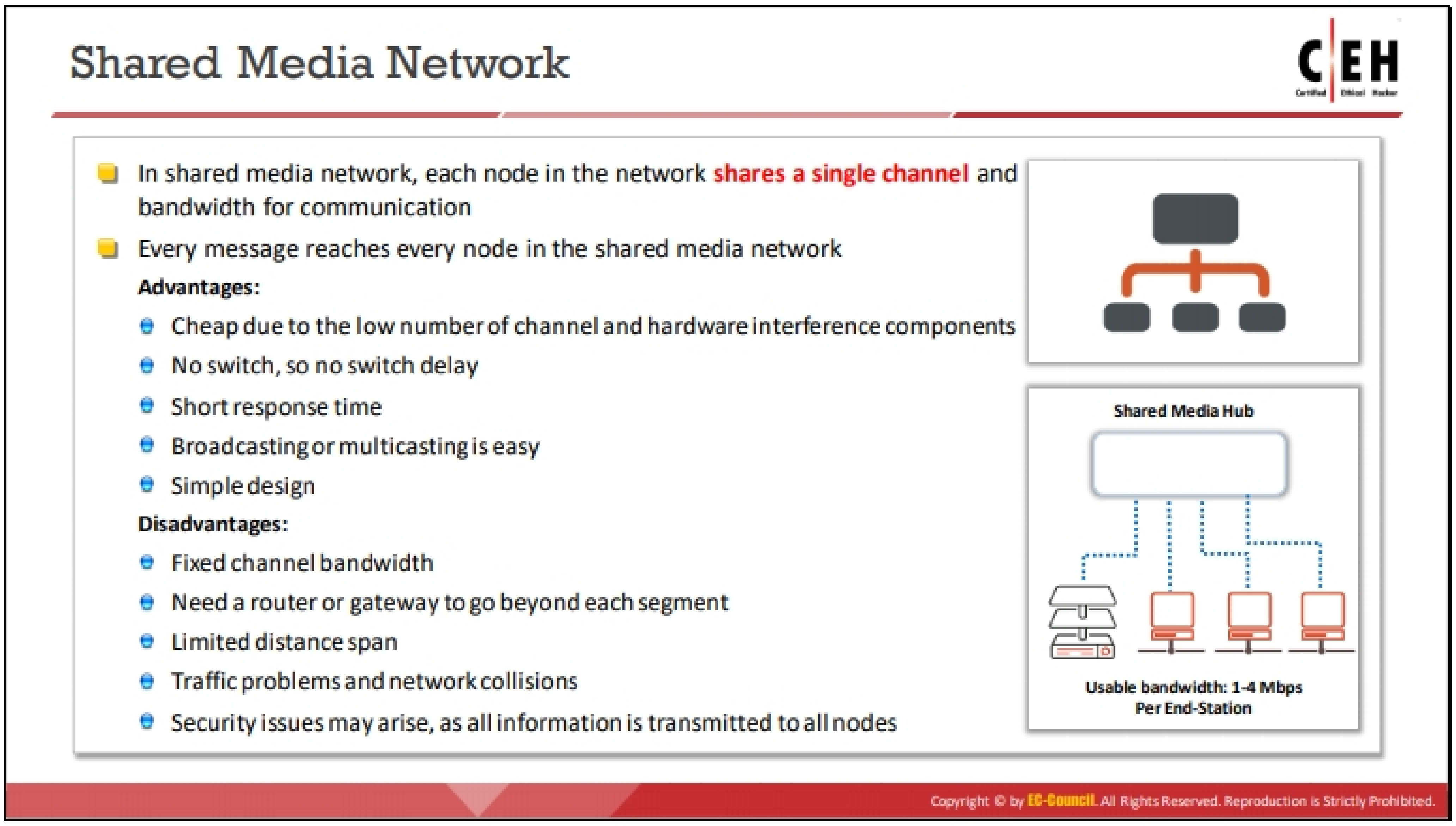
- The number of devices for a specific network topology is reduced
- Managing physical devices becomes less complex
- Increases security options through separation and specific frame delivery
- Performance and security
- Formation of virtual workgroups
- Simplified administration

Disadvantages:

- VLANS rely on switches to do right thing
- Packet leaks from one VLAN to the text
- Injected packets meant for an attack

Security implications of VLANs

- Keeps hosts separated by VLANS and limits the number of devices that can talk to these hosts
- Increases security options via separation and specific frame delivery
- Controls inter-VLAN routing using IP access lists
- Deploys VTP domain, VTP pruning, and password protections



Shared Media Network

- In shared media network, each node in the network **shares a single channel** and bandwidth for communication
- Every message reaches every node in the shared media network

Advantages:

- Cheap due to the low number of channel and hardware interference components
- No switch, so no switch delay
- Short response time
- Broadcasting or multicasting is easy
- Simple design

Disadvantages:

- Fixed channel bandwidth
- Need a router or gateway to go beyond each segment
- Limited distance span
- Traffic problems and network collisions
- Security issues may arise, as all information is transmitted to all nodes

Notes:

Switched Media Network

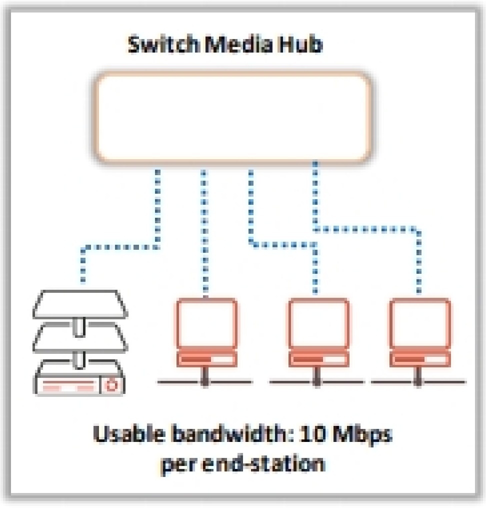
- In a switched media network, **point-to-point communication** is established through a dedicated line
- The communication needs switches to establish direct connection

Advantages:

- High bandwidth so that multiple pairs of nodes can communicate simultaneously
- No collision

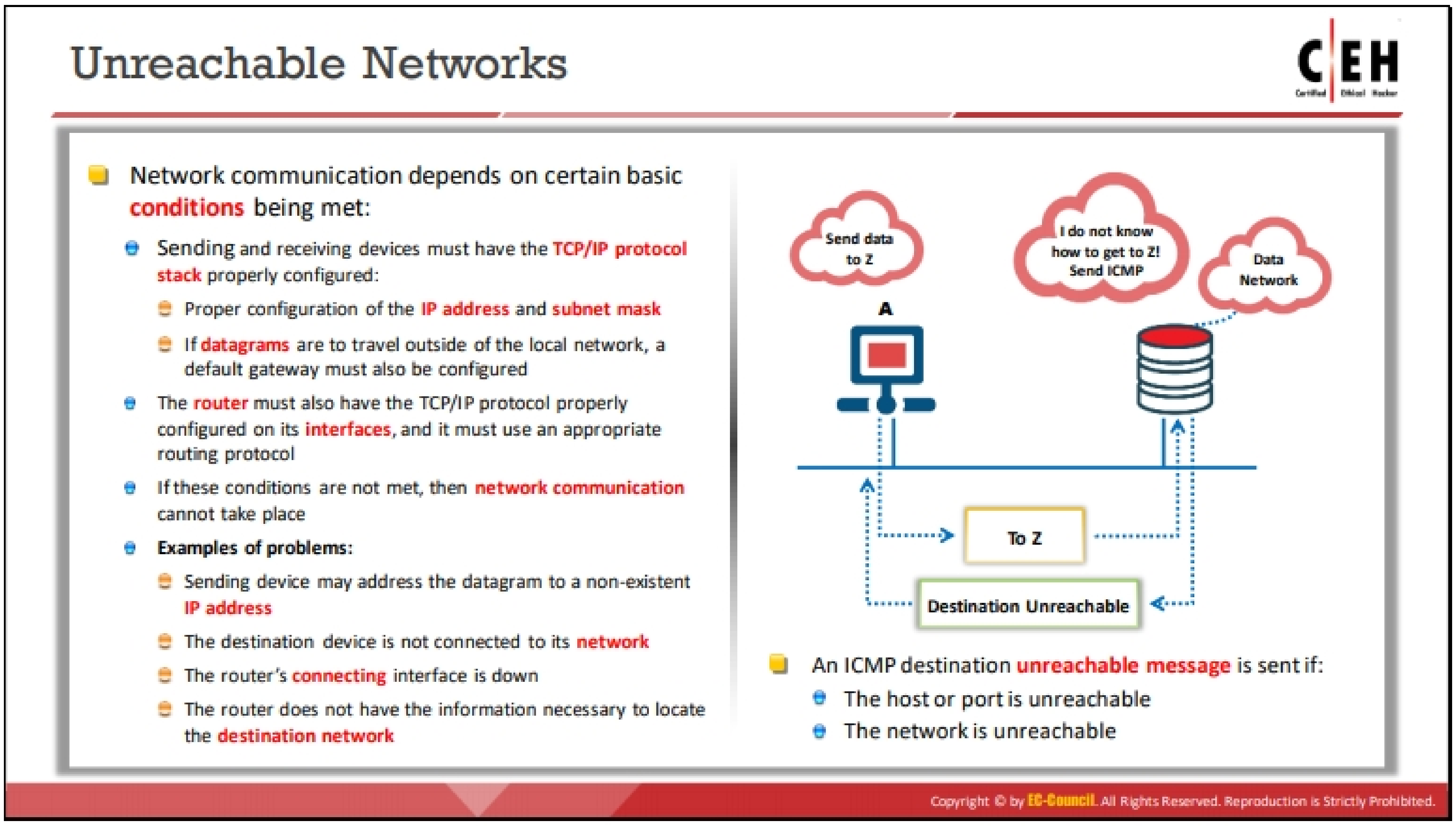
Disadvantages:

- Expensive
- Complex design
- Long response time
- Security issues arise if the port is enabled on access switches. Rogue devices can provide access to the network



Basic Network Troubleshooting

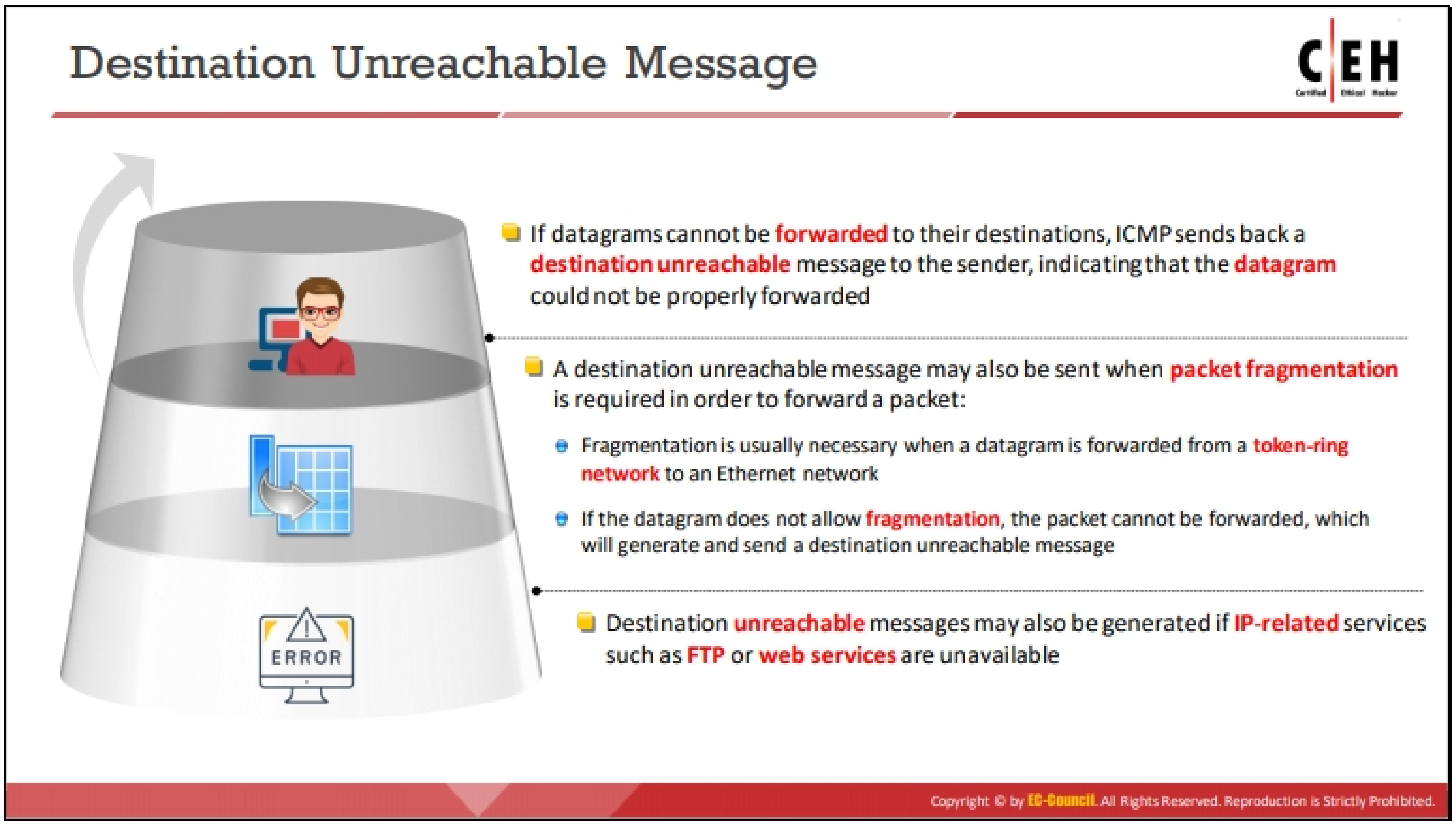
Notes:



Unreachable Networks

- Network communication depends on certain basic **conditions** being met:
  - Sending and receiving devices must have the **TCP/IP protocol stack** properly configured:
    - Proper configuration of the **IP address** and **subnet mask**
    - If **datagrams** are to travel outside of the local network, a default gateway must also be configured
  - The **router** must also have the TCP/IP protocol properly configured on its **interfaces**, and it must use an appropriate routing protocol
  - If these conditions are not met, then **network communication** cannot take place
  - **Examples of problems:**
    - Sending device may address the datagram to a non-existent **IP address**
    - The destination device is not connected to its **network**
    - The router's **connecting** interface is down
    - The router does not have the information necessary to locate the **destination network**

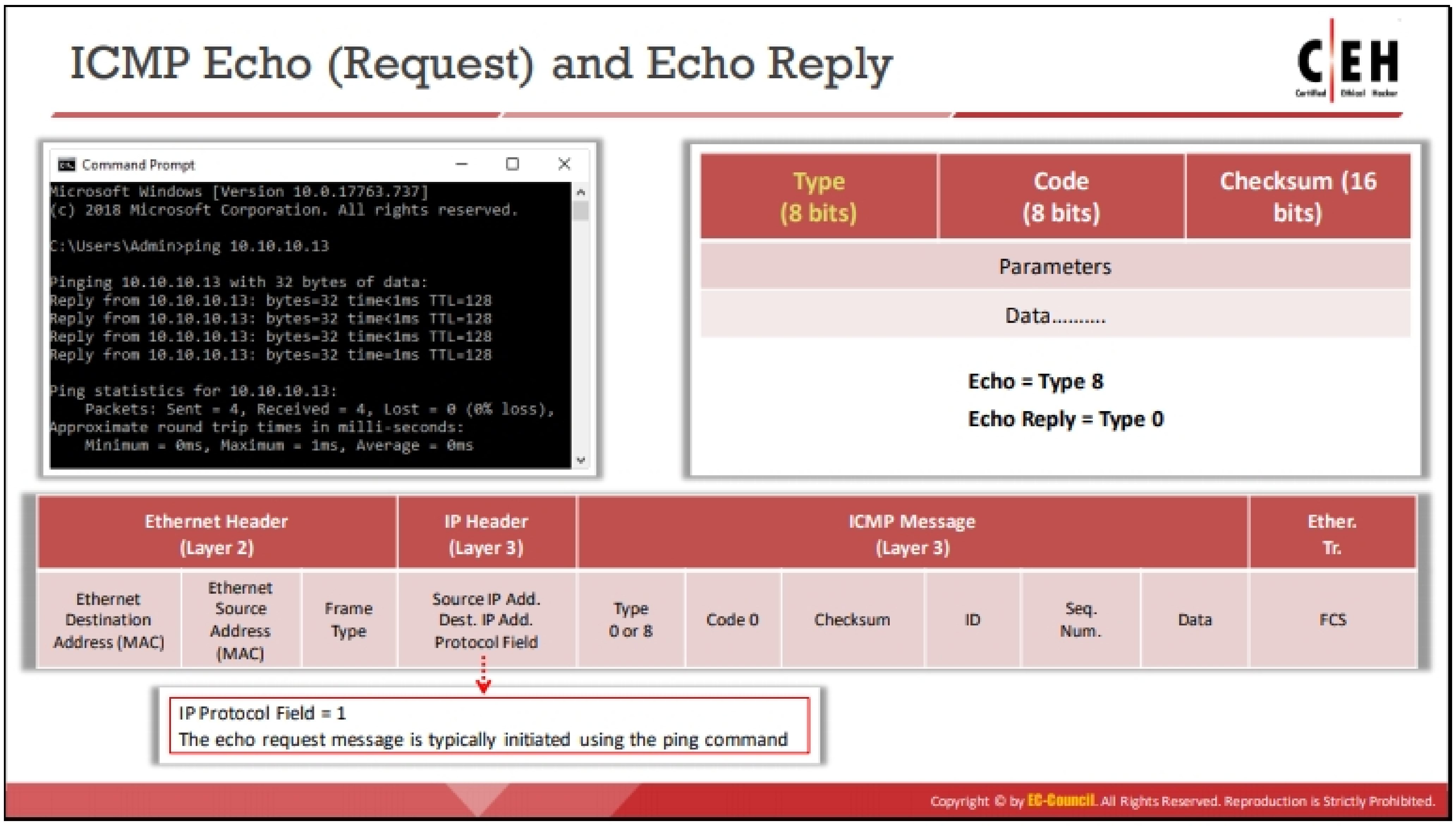
- An ICMP destination **unreachable message** is sent if:
  - The host or port is unreachable
  - The network is unreachable



Destination Unreachable Message

- If datagrams cannot be **forwarded** to their destinations, ICMP sends back a **destination unreachable** message to the sender, indicating that the **datagram** could not be properly forwarded
- A destination unreachable message may also be sent when **packet fragmentation** is required in order to forward a packet:
  - Fragmentation is usually necessary when a datagram is forwarded from a **token-ring network** to an Ethernet network
  - If the datagram does not allow **fragmentation**, the packet cannot be forwarded, which will generate and send a destination unreachable message
- Destination **unreachable** messages may also be generated if **IP-related** services such as **FTP** or **web services** are unavailable

Notes: ____



ICMP Echo (Request) and Echo Reply

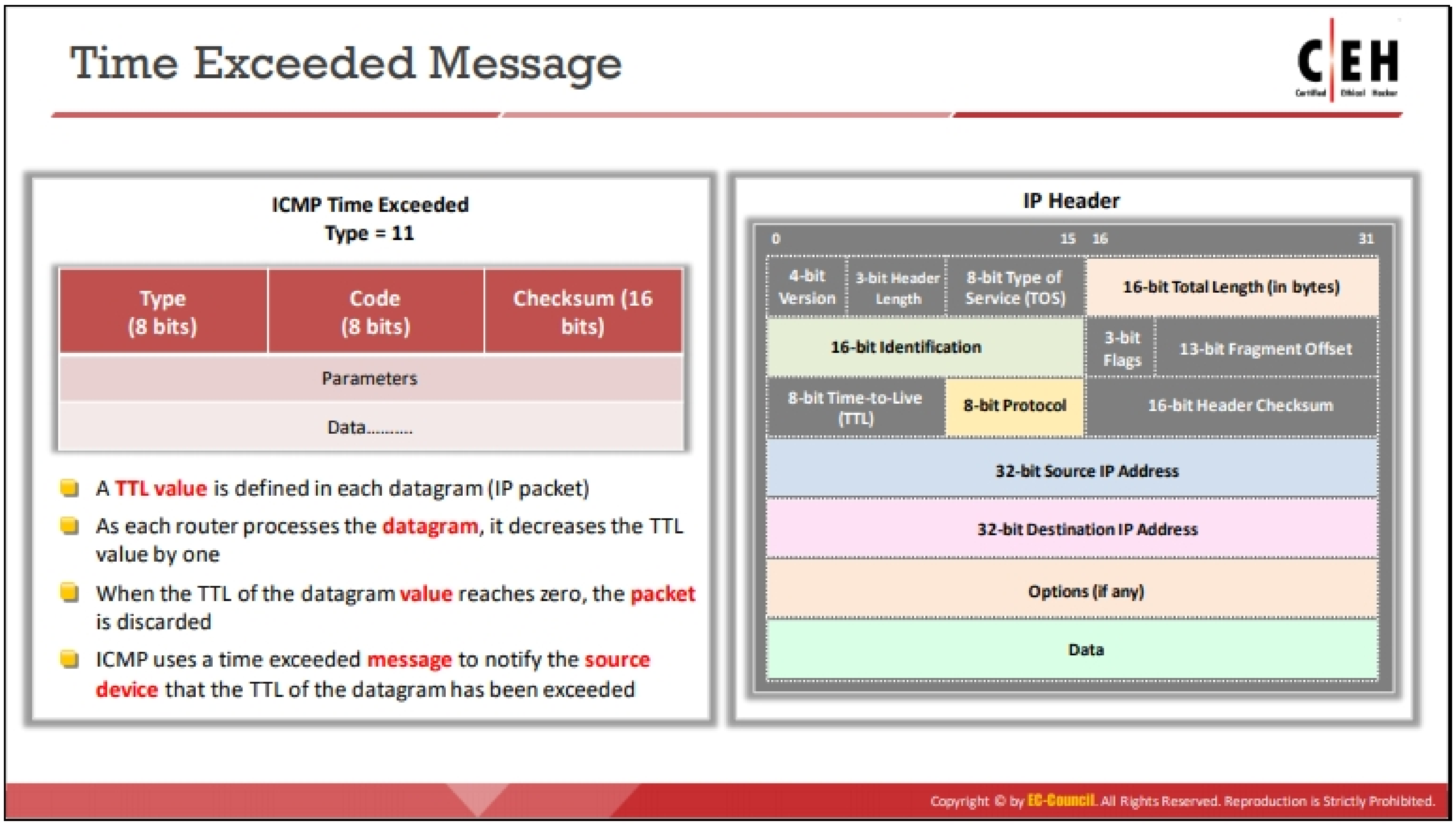
```
Microsoft Windows [Version 10.0.17763.737]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Users\Admin>ping 10.10.10.13

Pinging 10.10.10.13 with 32 bytes of data:
Reply from 10.10.10.13: bytes=32 time<1ms TTL=128
Reply from 10.10.10.13: bytes=32 time<1ms TTL=128
Reply from 10.10.10.13: bytes=32 time<1ms TTL=128
Reply from 10.10.10.13: bytes=32 time=1ms TTL=128

Ping statistics for 10.10.10.13:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms
```

Type (8 bits)	Code (8 bits)	Checksum (16 bits)
Parameters		
Data..........		

Echo = Type 8
Echo Reply = Type 0

Ethernet Header (Layer 2)			IP Header (Layer 3)	ICMP Message (Layer 3)						Ether. Tr.
Ethernet Destination Address (MAC)	Ethernet Source Address (MAC)	Frame Type	Source IP Add. Dest. IP Add. Protocol Field	Type 0 or 8	Code 0	Checksum	ID	Seq. Num.	Data	FCS

IP Protocol Field = 1
The echo request message is typically initiated using the ping command



Time Exceeded Message

ICMP Time Exceeded
Type = 11

Type (8 bits)	Code (8 bits)	Checksum (16 bits)
Parameters		
Data..........		

- A TTL value is defined in each datagram (IP packet)
- As each router processes the datagram, it decreases the TTL value by one
- When the TTL of the datagram value reaches zero, the packet is discarded
- ICMP uses a time exceeded message to notify the source device that the TTL of the datagram has been exceeded

IP Header

0		15	16	31
4-bit Version	3-bit Header Length	8-bit Type of Service (TOS)	16-bit Total Length (in bytes)	
16-bit Identification			3-bit Flags	13-bit Fragment Offset
8-bit Time-to-Live (TTL)		8-bit Protocol	16-bit Header Checksum	
32-bit Source IP Address				
32-bit Destination IP Address				
Options (if any)				
Data				

Notes: ____

____

____

____

____

____

IP Parameter Problem

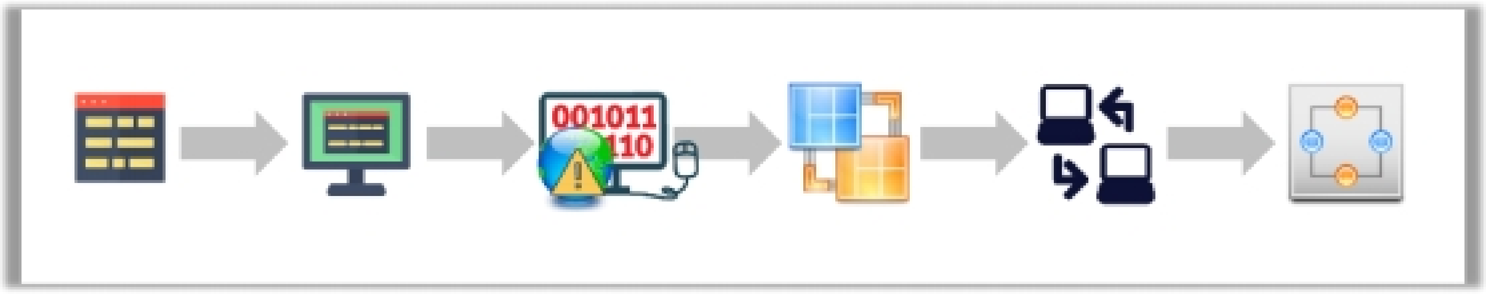
- Devices that **process** datagrams may not be able to forward them due to some type of **error** in the header
- Such errors do not relate to the state of the destination **host** or network, but still prevent the datagram from being **processed** and **delivered**
- An ICMP **type 12 parameter** problem message is sent to the **source** of the **datagram**

ICMP Parameter Problem
Type = 12

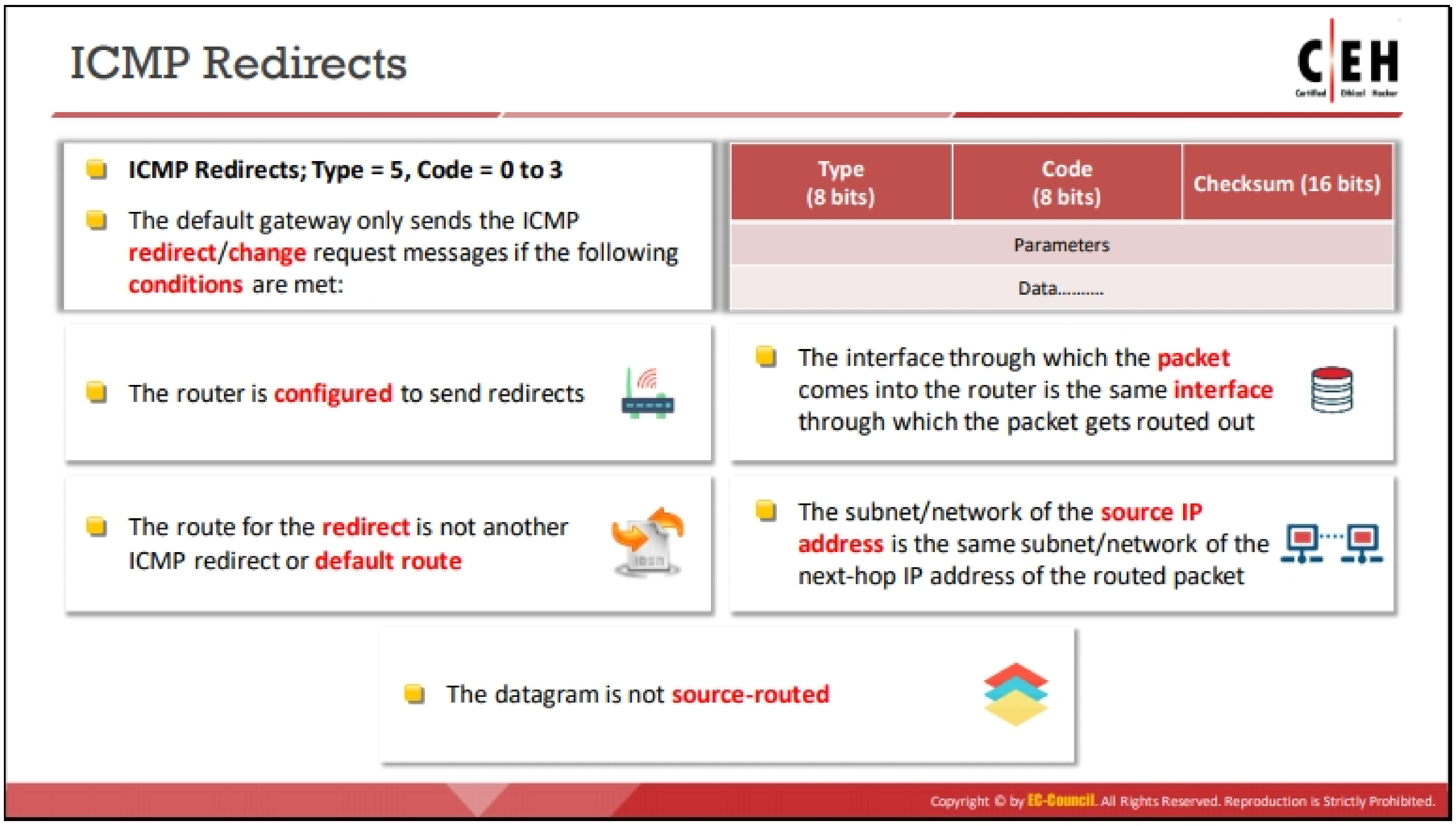
0	8	16	31
Type (3)	Code (0-12)	Checksum	
Unused (must be zero)			
Internet Header + First 64 Bits of Datagram			

ICMP Control Messages

- Unlike error messages, control messages are not the result of **lost packets** or error conditions that occur during packet transmission
- Instead, they are used to inform **hosts** of conditions such as:
  - Network **congestion**
  - The existence of a better **gateway** to a remote network



Notes: ____

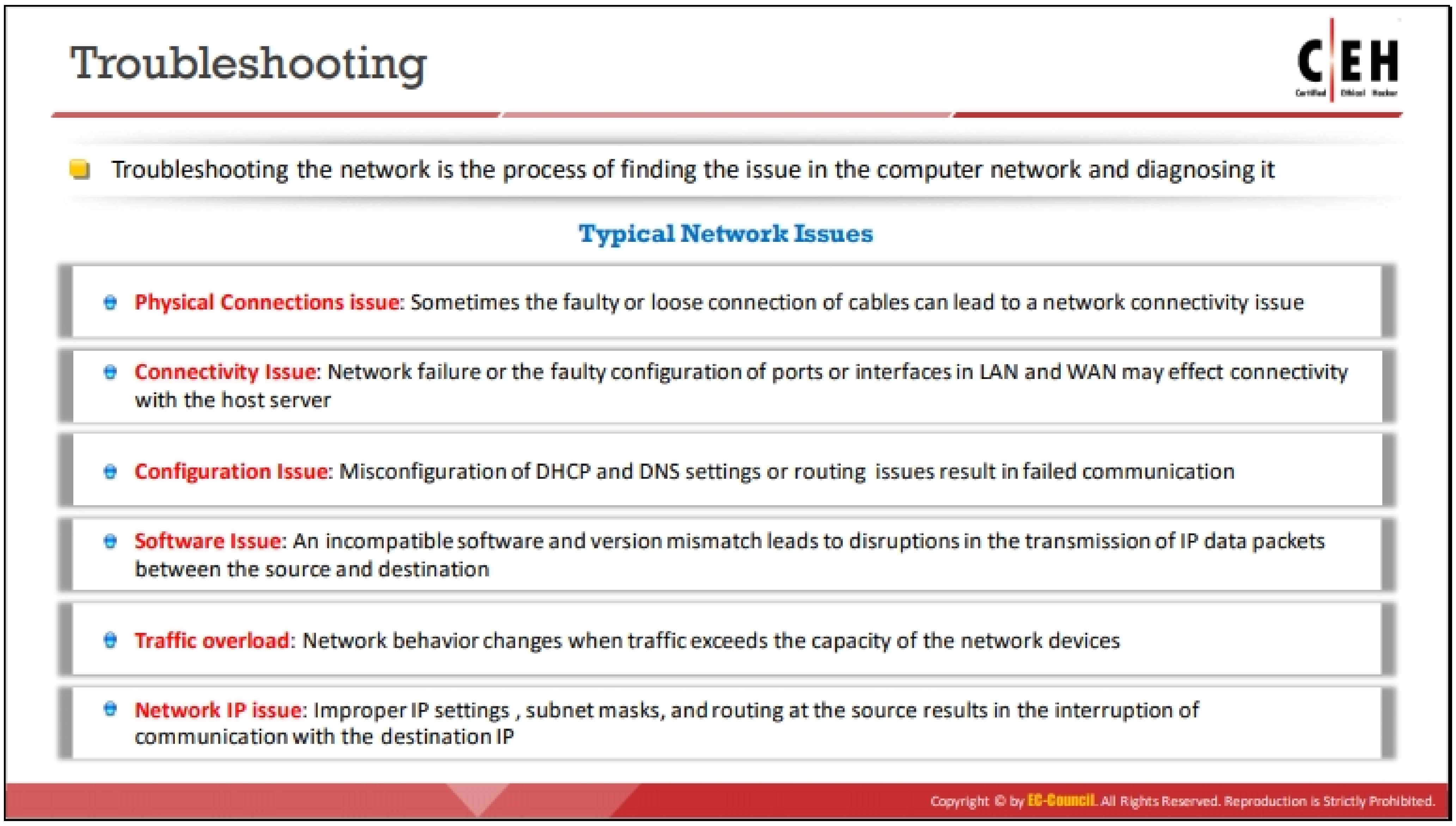


ICMP Redirects

- **ICMP Redirects; Type = 5, Code = 0 to 3**
- The default gateway only sends the ICMP **redirect**/**change** request messages if the following **conditions** are met:

Type (8 bits)	Code (8 bits)	Checksum (16 bits)
Parameters		
Data..........		

- The router is **configured** to send redirects
- The interface through which the **packet** comes into the router is the same **interface** through which the packet gets routed out
- The route for the **redirect** is not another ICMP redirect or **default route**
- The subnet/network of the **source IP address** is the same subnet/network of the next-hop IP address of the routed packet
- The datagram is not **source-routed**



Troubleshooting

- Troubleshooting the network is the process of finding the issue in the computer network and diagnosing it

Typical Network Issues

- **Physical Connections issue**: Sometimes the faulty or loose connection of cables can lead to a network connectivity issue
- **Connectivity Issue**: Network failure or the faulty configuration of ports or interfaces in LAN and WAN may effect connectivity with the host server
- **Configuration Issue**: Misconfiguration of DHCP and DNS settings or routing issues result in failed communication
- **Software Issue**: An incompatible software and version mismatch leads to disruptions in the transmission of IP data packets between the source and destination
- **Traffic overload**: Network behavior changes when traffic exceeds the capacity of the network devices
- **Network IP issue**: Improper IP settings , subnet masks, and routing at the source results in the interruption of communication with the destination IP

Notes: ____

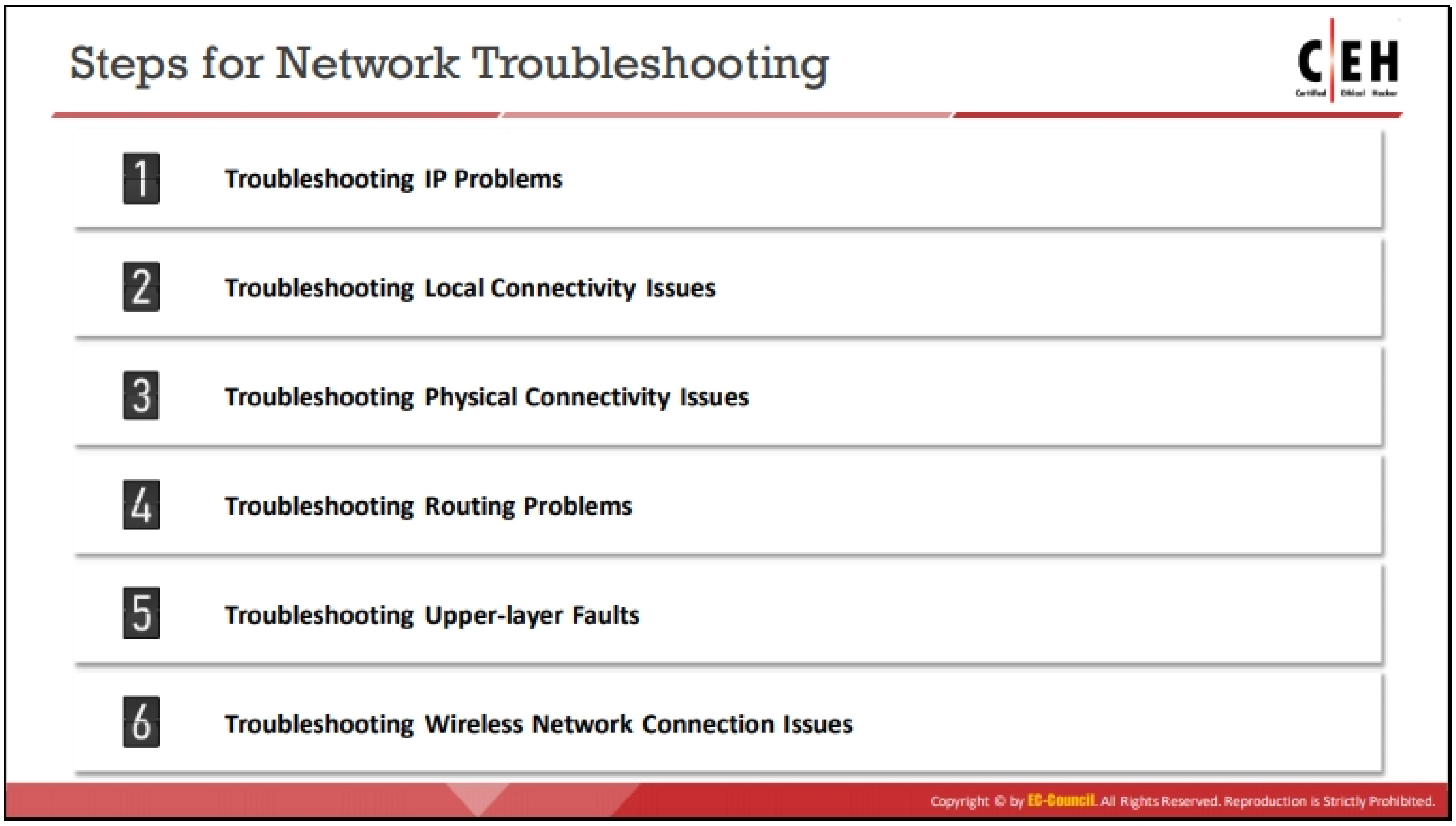
____

____

____

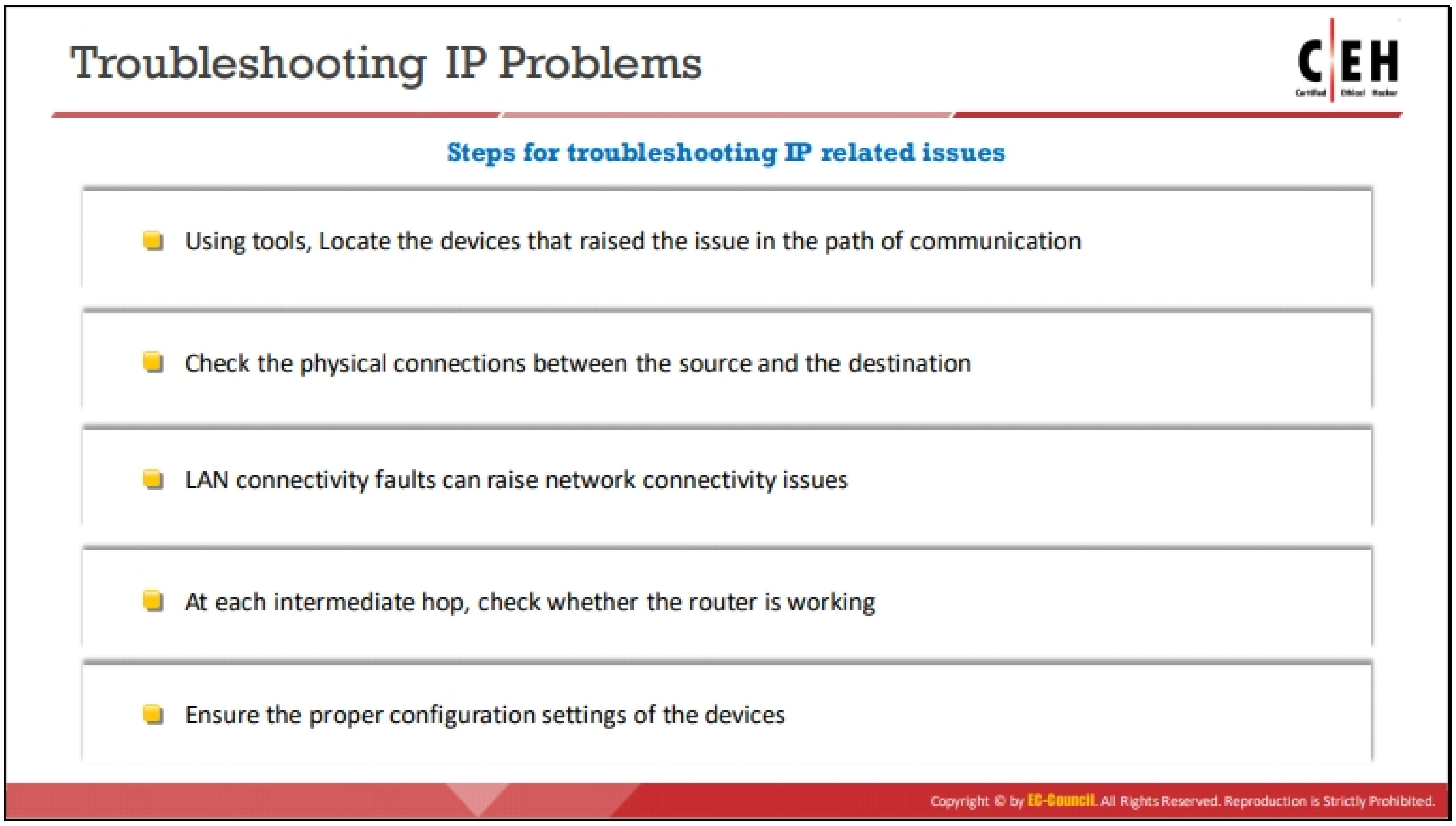
____

____



Steps for Network Troubleshooting

1. **Troubleshooting IP Problems**
2. **Troubleshooting Local Connectivity Issues**
3. **Troubleshooting Physical Connectivity Issues**
4. **Troubleshooting Routing Problems**
5. **Troubleshooting Upper-layer Faults**
6. **Troubleshooting Wireless Network Connection Issues**

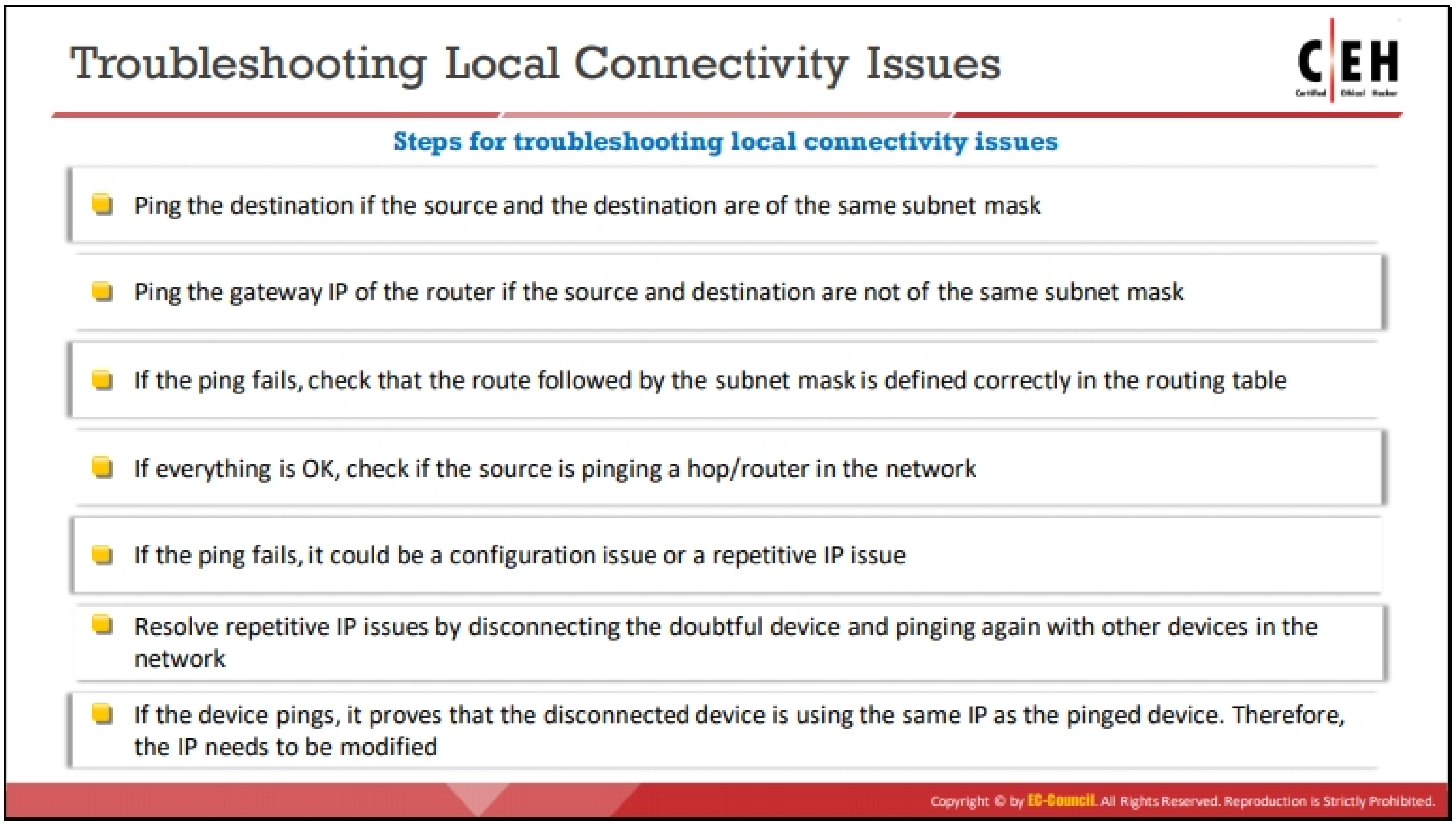


Troubleshooting IP Problems

Steps for troubleshooting IP related issues

- Using tools, Locate the devices that raised the issue in the path of communication
- Check the physical connections between the source and the destination
- LAN connectivity faults can raise network connectivity issues
- At each intermediate hop, check whether the router is working
- Ensure the proper configuration settings of the devices

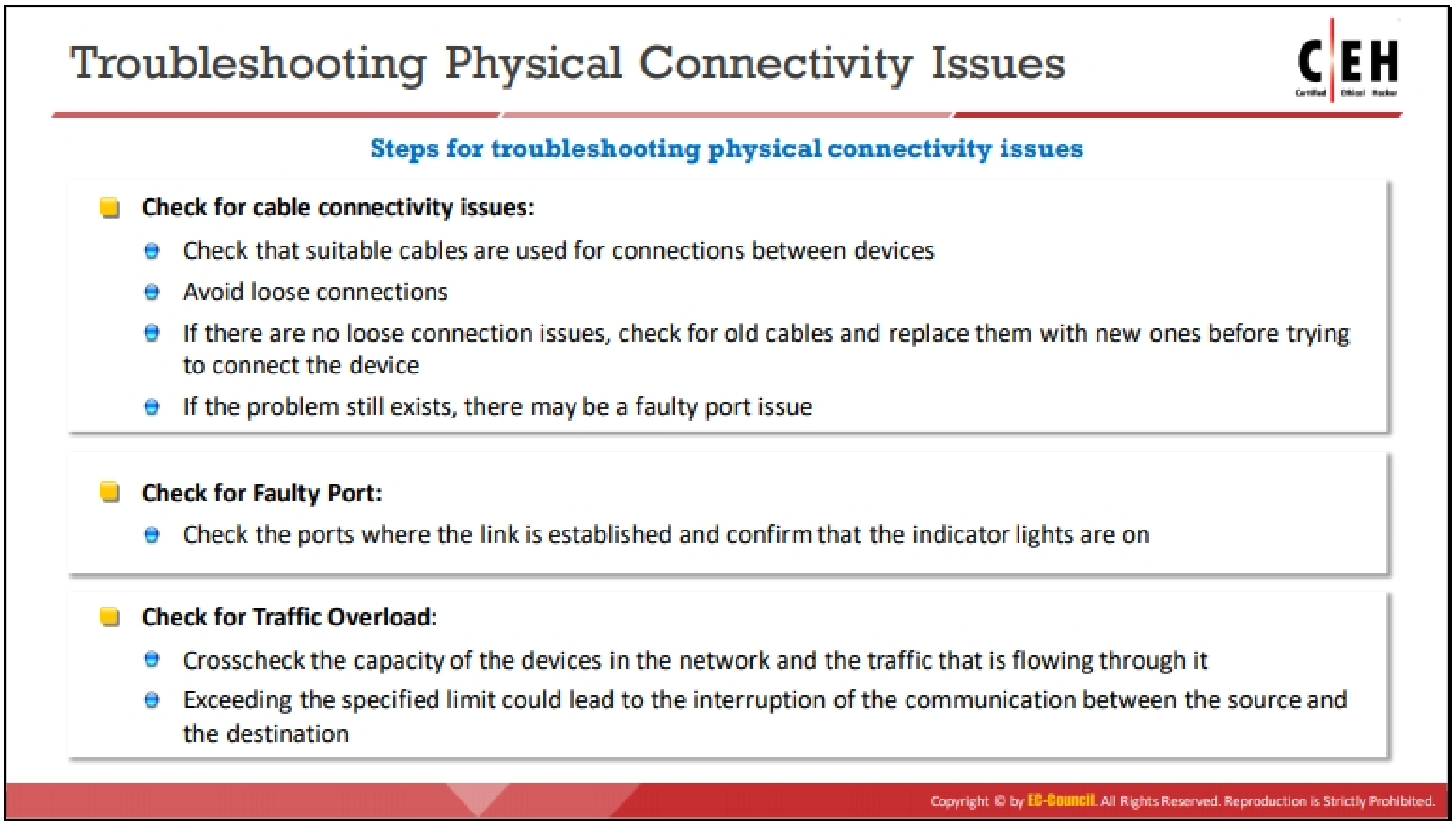
Notes: ______________________________



Troubleshooting Local Connectivity Issues

Steps for troubleshooting local connectivity issues

- Ping the destination if the source and the destination are of the same subnet mask
- Ping the gateway IP of the router if the source and destination are not of the same subnet mask
- If the ping fails, check that the route followed by the subnet mask is defined correctly in the routing table
- If everything is OK, check if the source is pinging a hop/router in the network
- If the ping fails, it could be a configuration issue or a repetitive IP issue
- Resolve repetitive IP issues by disconnecting the doubtful device and pinging again with other devices in the network
- If the device pings, it proves that the disconnected device is using the same IP as the pinged device. Therefore, the IP needs to be modified

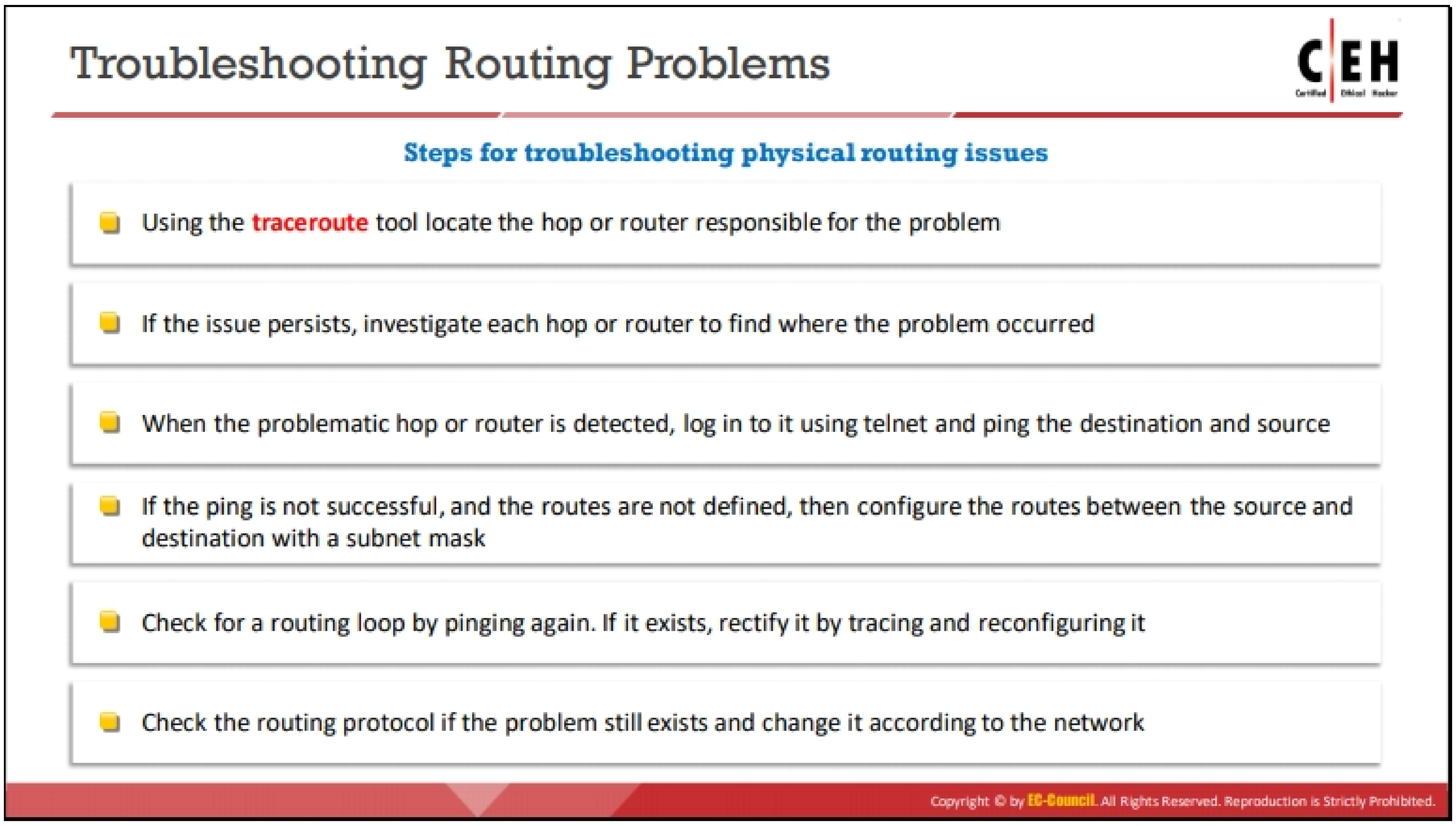


Troubleshooting Physical Connectivity Issues

Steps for troubleshooting physical connectivity issues

- **Check for cable connectivity issues:**
  - Check that suitable cables are used for connections between devices
  - Avoid loose connections
  - If there are no loose connection issues, check for old cables and replace them with new ones before trying to connect the device
  - If the problem still exists, there may be a faulty port issue
- **Check for Faulty Port:**
  - Check the ports where the link is established and confirm that the indicator lights are on
- **Check for Traffic Overload:**
  - Crosscheck the capacity of the devices in the network and the traffic that is flowing through it
  - Exceeding the specified limit could lead to the interruption of the communication between the source and the destination

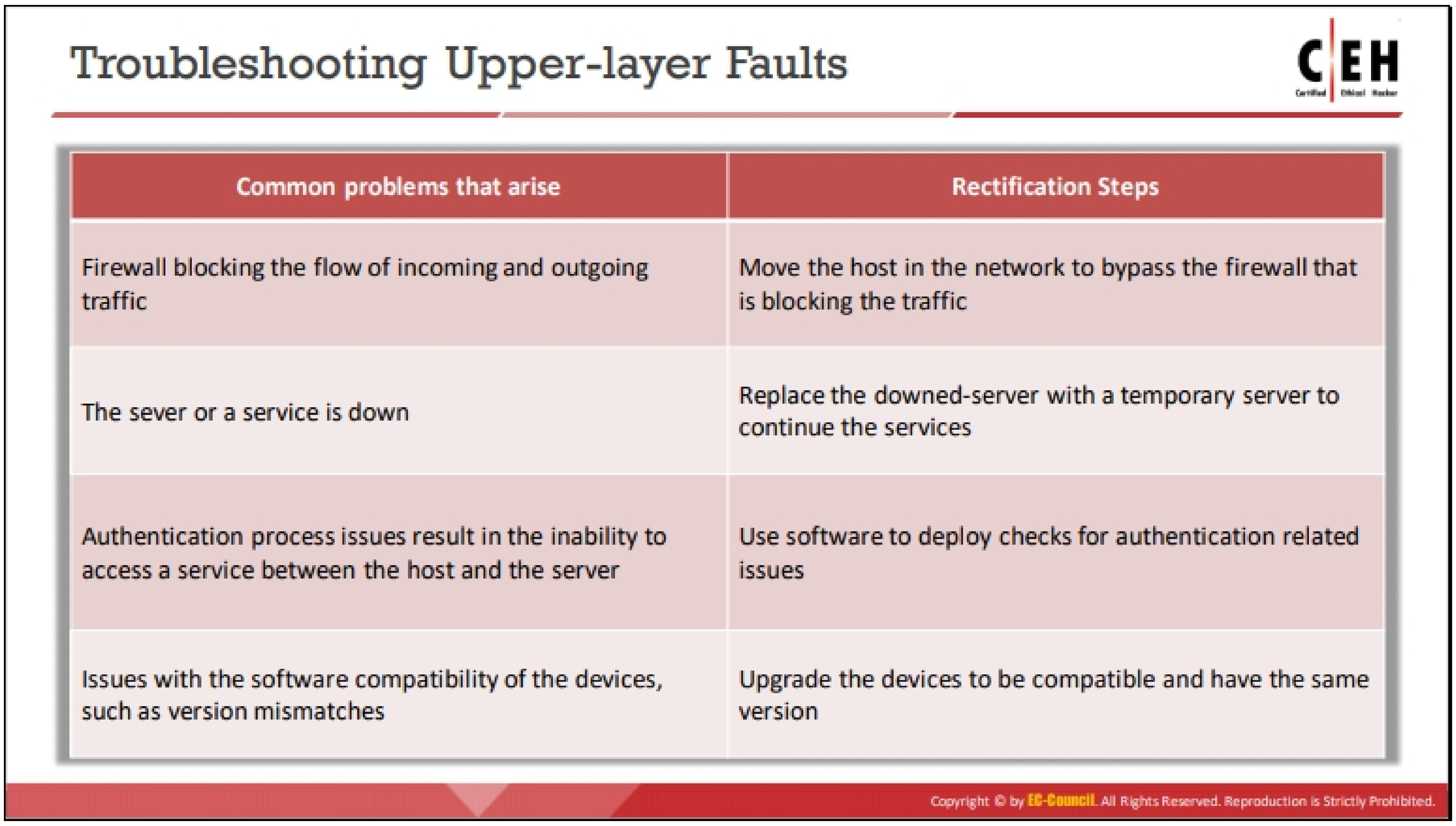
Notes:



Troubleshooting Routing Problems

Steps for troubleshooting physical routing issues

- Using the traceroute tool locate the hop or router responsible for the problem
- If the issue persists, investigate each hop or router to find where the problem occurred
- When the problematic hop or router is detected, log in to it using telnet and ping the destination and source
- If the ping is not successful, and the routes are not defined, then configure the routes between the source and destination with a subnet mask
- Check for a routing loop by pinging again. If it exists, rectify it by tracing and reconfiguring it
- Check the routing protocol if the problem still exists and change it according to the network



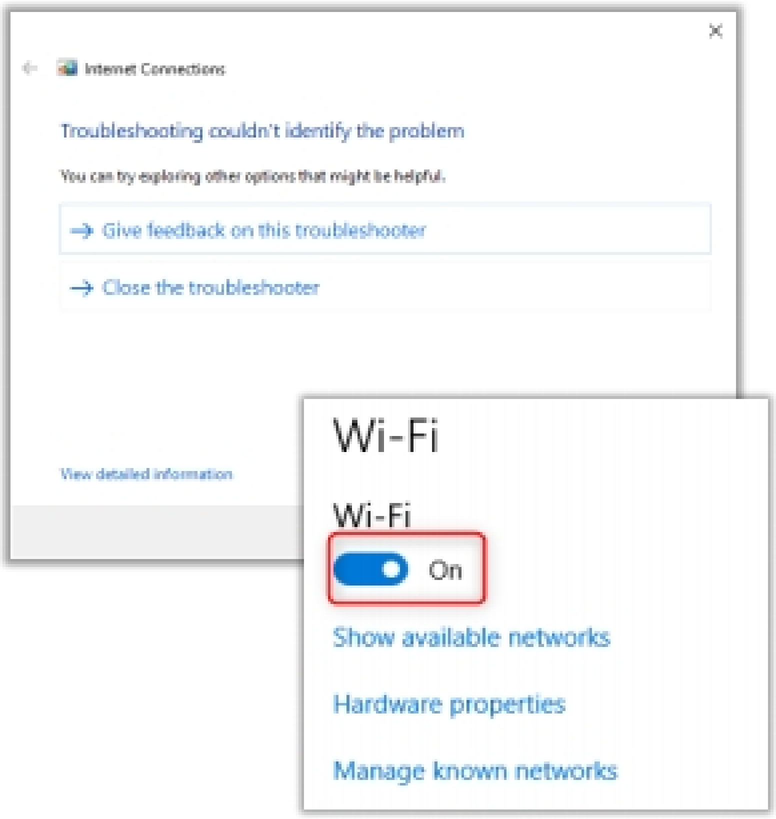
Troubleshooting Upper-layer Faults

Common problems that arise	Rectification Steps
Firewall blocking the flow of incoming and outgoing traffic	Move the host in the network to bypass the firewall that is blocking the traffic
The sever or a service is down	Replace the downed-server with a temporary server to continue the services
Authentication process issues result in the inability to access a service between the host and the server	Use software to deploy checks for authentication related issues
Issues with the software compatibility of the devices, such as version mismatches	Upgrade the devices to be compatible and have the same version

Notes: ____

Troubleshooting Wireless Network Connection Issues

- Check whether the Wi-Fi is enabled on the devices
- To check, Go to **Settings → Network & Internet → Wi-Fi**
- If the problem still exists, check and change the SSID and access points to allocate an IP to the requesting device
- Use the **Windows Network Diagnostics** tool to troubleshoot the network related issue
- **Windows Network Diagnostics** will troubleshoot to the detect the problem by downloading and installing available patches
- Restore the router to its factory settings and restart it



Internet Connections

Troubleshooting couldn't identify the problem

You can try exploring other options that might be helpful.

→ Give feedback on this troubleshooter

→ Close the troubleshooter

View detailed information

Wi-Fi

Wi-Fi

On

Show available networks

Hardware properties

Manage known networks

Network Troubleshooting Tools

List of basic network troubleshooting utilities and tools

- **Ping**
- **Tracert/traceroute**
- **Ipconfig/ifconfig**
- **NSlookup**
- **Netstat**
- **PuTTY/Tera Term**
- **Subnet and IP Calculator**
- **Speedtest.net**
- **Pathping/mtr**
- **Route**

Notes: ____

____

____

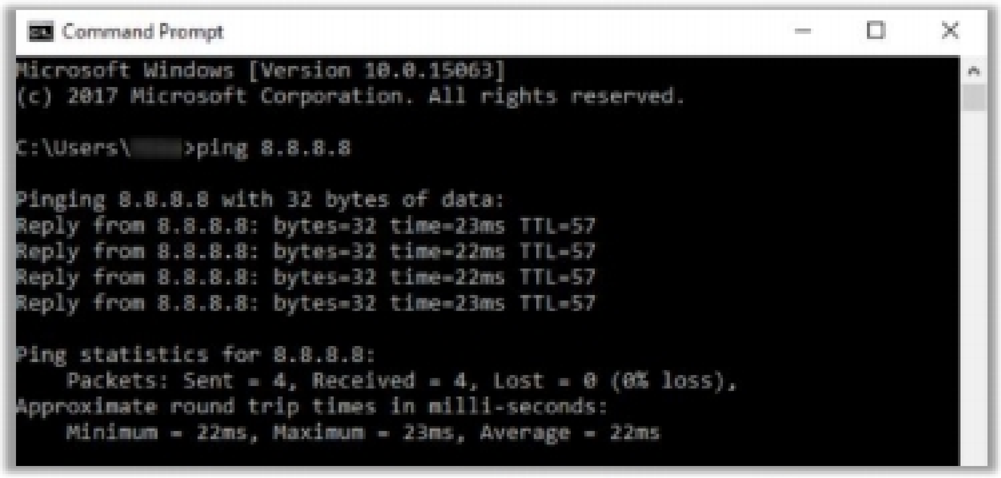
____

____

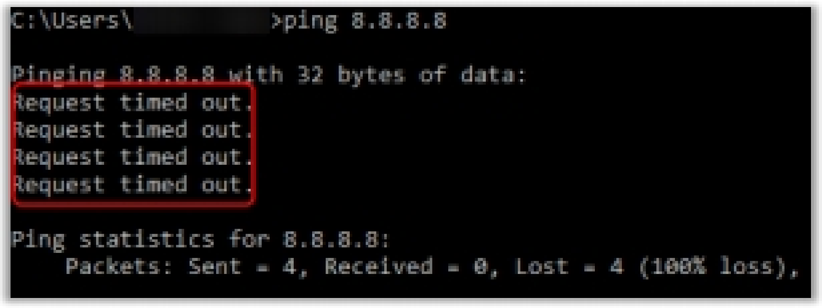
____

Ping

- The ping utility is used to test if an IP address or a website is accessible by the host
- When a reply is received from the pinged IP address, it shows that the packets are transferring between the system and the given IP
  - Launch the command prompt and execute `ping x.x.x.x` or `ping example.com` to check the availability of the host to the computer
  - "Request timed out" shows that there is no connection between the system and the host, or that the system is unable to connect to the host



```
Microsoft Windows [Version 10.0.15063]
(c) 2017 Microsoft Corporation. All rights reserved.

C:\Users\[redacted]>ping 8.8.8.8

Pinging 8.8.8.8 with 32 bytes of data:
Reply from 8.8.8.8: bytes=32 time=23ms TTL=57
Reply from 8.8.8.8: bytes=32 time=22ms TTL=57
Reply from 8.8.8.8: bytes=32 time=22ms TTL=57
Reply from 8.8.8.8: bytes=32 time=23ms TTL=57

Ping statistics for 8.8.8.8:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 22ms, Maximum = 23ms, Average = 22ms
```

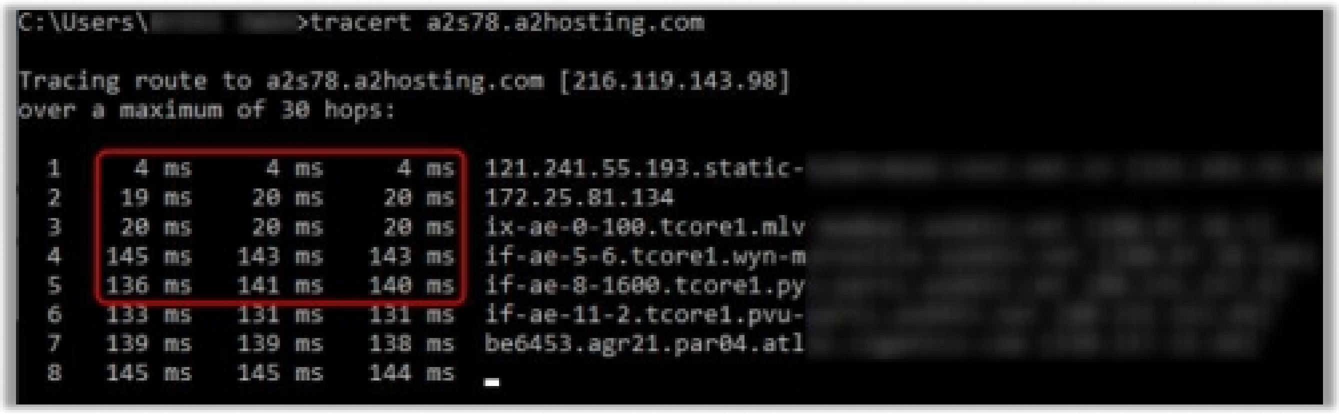


```
C:\Users\[redacted]>ping 8.8.8.8

Pinging 8.8.8.8 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 8.8.8.8:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

Traceroute and Tracert

- The **Traceroute** utility is used to trace packets across a network and to understand connections to a server
- Traceroute sends an ICMP echo request message to the specified destination
- If the destination is active, it sends ICMP echo reply messages as a response, which confirms the connection is active
- If not, the destination may be inactive, or there could be a connectivity issue with the source

- Use the `tracert` command along with the hostname of the computer to which the route must be traced
- Each hop is indicated by a number in the left column, along with the domain and the IP address



```
C:\Users\[redacted]>tracert a2s78.a2hosting.com

Tracing route to a2s78.a2hosting.com [216.119.143.98]
over a maximum of 30 hops:

  1     4 ms     4 ms     4 ms  121.241.55.193.static-[redacted]
  2    19 ms    20 ms    20 ms  172.25.81.134
  3    20 ms    20 ms    20 ms  ix-ae-0-100.tcore1.mlv
  4   145 ms   143 ms   143 ms  if-ae-5-6.tcore1.wyn-m
  5   136 ms   141 ms   140 ms  if-ae-8-1600.tcore1.py
  6   133 ms   131 ms   131 ms  if-ae-11-2.tcore1.pvu-
  7   139 ms   139 ms   138 ms  be6453.agr21.par04.atl
  8   145 ms   145 ms   144 ms  _
```

Notes: ____

____

____

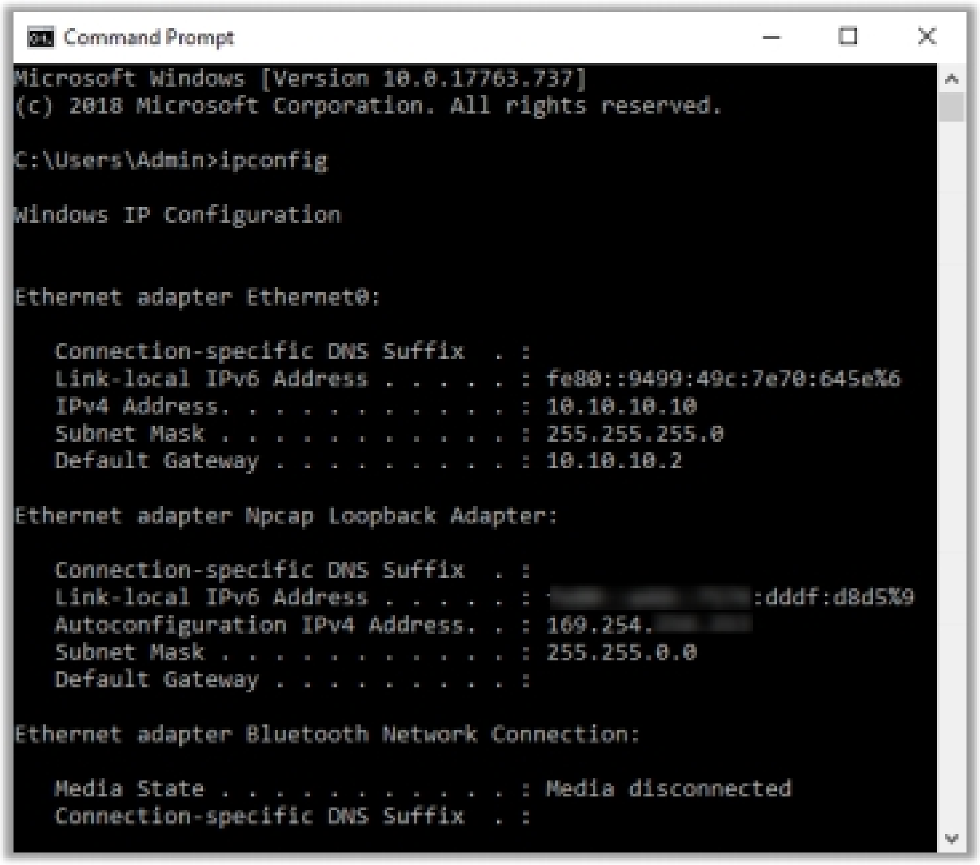
____

____

____

Ipconfig and Ifconfig

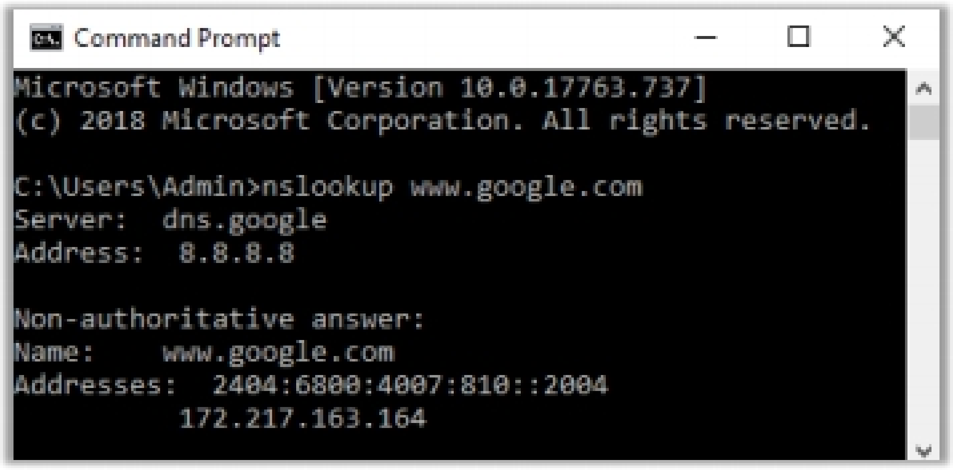
- **Ipconfig (Internet protocol configuration)** is a command line utility used to display all current TCP/IP network configuration values along with the IP address, subnet mask, and default gateway for all adapters
  - To display the basic configuration of the system, use `ipconfig` in the command prompt terminal
  - For a detailed information on the system configuration, execute `ipconfig /all` in the command prompt
  - **Ifconfig** is a similar utility for Linux-based machines



```
Microsoft Windows [Version 10.0.17763.737]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Users\Admin>ipconfig

Windows IP Configuration


Ethernet adapter Ethernet0:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::9499:49c:7e70:645e%6
   IPv4 Address. . . . . . . . . . . : 10.10.10.10
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 10.10.10.2

Ethernet adapter Npcap Loopback Adapter:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : [redacted]:dddf:d8d5%9
   Autoconfiguration IPv4 Address. . : 169.254.[redacted]
   Subnet Mask . . . . . . . . . . . : 255.255.0.0
   Default Gateway . . . . . . . . . :

Ethernet adapter Bluetooth Network Connection:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :
```

NSlookup

- **NSlookup** utility is used to lookup a specific IP address or multiple IP addresses associated with a domain name
- NSlookup is used when a user can access a resource by specifying its IP address, but cannot access it by its **DNS** name
- Nslookup utility is used to fix DNS address resolution issues
- The `nslookup` command is executed in the command prompt to lookup the IP address for a DNS name
- Subcommands can be used at the end of the nslookup command to perform queries or set options



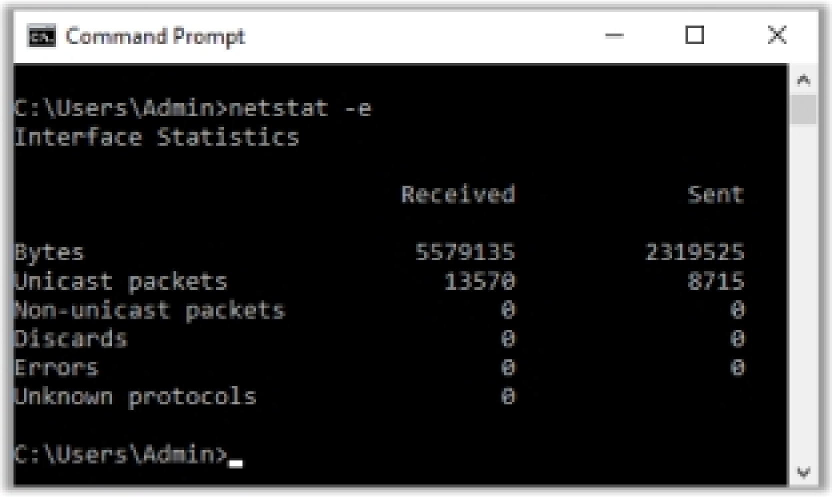
```
Microsoft Windows [Version 10.0.17763.737]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Users\Admin>nslookup www.google.com
Server:  dns.google
Address:  8.8.8.8

Non-authoritative answer:
Name:    www.google.com
Addresses:  2404:6800:4007:810::2004
          172.217.163.164
```

Notes:

Netstat

- **Netstat** is a command line utility used to display both the incoming and outgoing traffic of TCP/IP
- Netstat can determine the current state of the active hosts on the network
- Netstat is used to identify the services associated with user defined ports

- Execute the `netstat` command without any parameters in the terminal to show the list of active connections
- Use the `netstat -e` command to show the statistics of various protocols

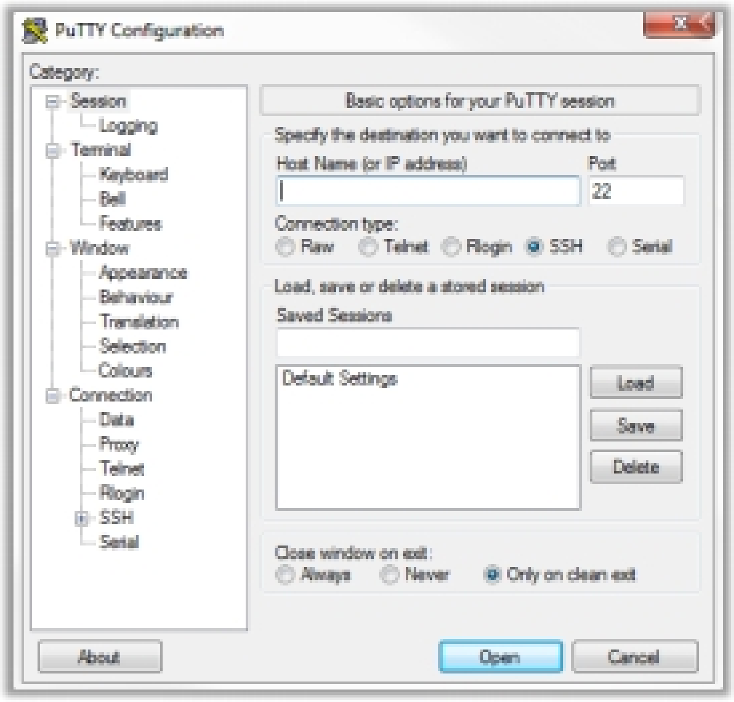

Command Prompt

```
C:\Users\Admin>netstat -e
Interface Statistics

                           Received            Sent

Bytes                       5579135         2319525
Unicast packets               13570            8715
Non-unicast packets               0               0
Discards                          0               0
Errors                            0               0
Unknown protocols                 0

C:\Users\Admin>_
```

PuTTY and Tera Term

- **PuTTY** is a tool used as a File Transfer Protocol or SFTP
- It generates hashes for passwords

- **Tera Term** is a tool used to automate tasks for remote connections. It supports telnet and SSH connections


PuTTY Configuration
Category:
Session
Logging
Terminal
Keyboard
Bell
Features
Window
Appearance
Behaviour
Translation
Selection
Colours
Connection
Data
Proxy
Telnet
Rlogin
SSH
Serial
Basic options for your PuTTY session
Load
Save
Delete
About
Open
Cancel

Specify the destination you want to connect to

Host Name (or IP address):

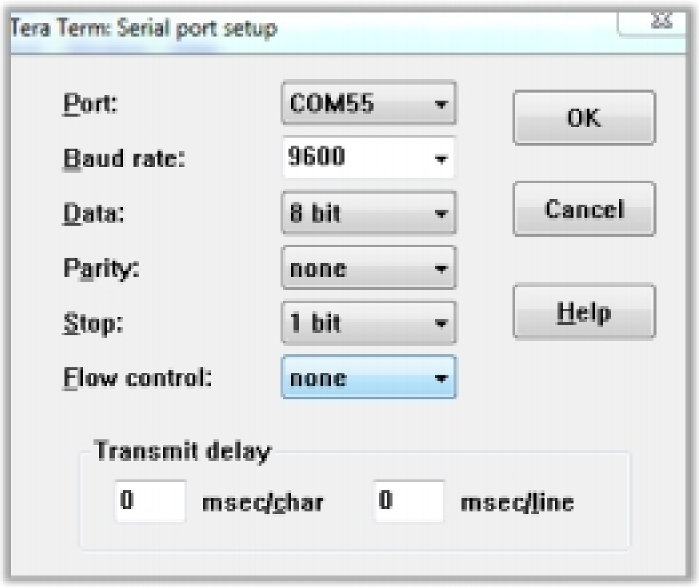
Port: 22

Connection type: ○ Raw ○ Telnet ○ Rlogin ● SSH ○ Serial

Load, save or delete a stored session

Saved Sessions: Default Settings

Close window on exit: ○ Always ○ Never ● Only on clean exit


Tera Term: Serial port setup
OK
Cancel
Help

Port: COM55

Baud rate: 9600

Data: 8 bit

Parity: none

Stop: 1 bit

Flow control: none

Transmit delay: 0 msec/char 0 msec/line

Notes: ____

____

____

____

____

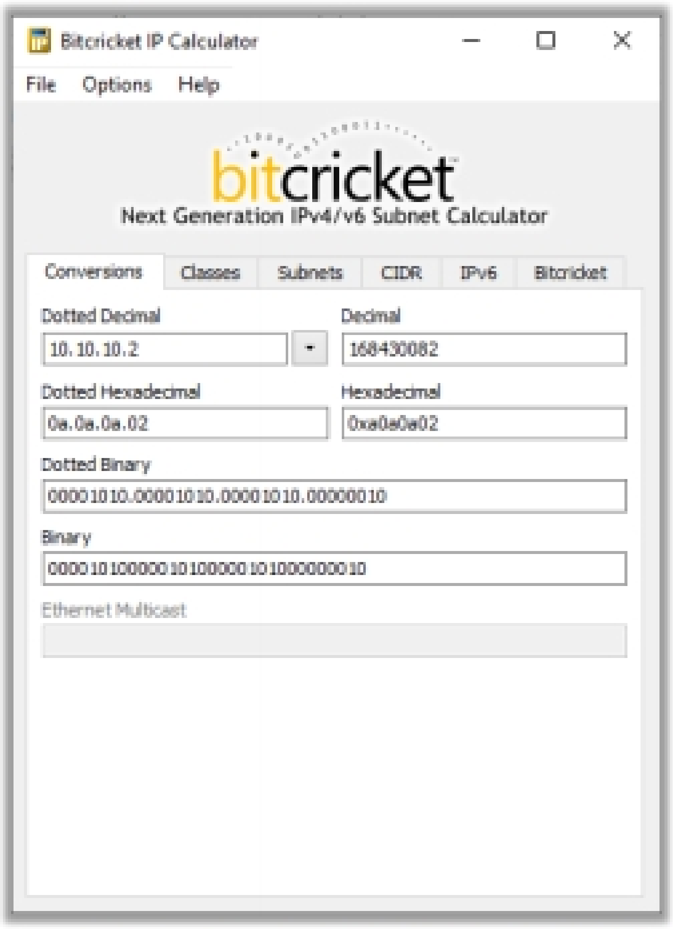
____

Subnet and IP Calculators

- The Subnet calculator is used to find out **information about IPv4**, IPv6 subnets. It is used for the division of classes of subnets
- The **IP calculator** is used to define possible IP addresses, along with the classes of IP
- Broadcast, network, and host ranges are calculated using the IP calculator
- The IP calculator and the Subnet calculator can be downloaded from the following links

http://www.bitcricket.com/downloads/IPCalculator.msi

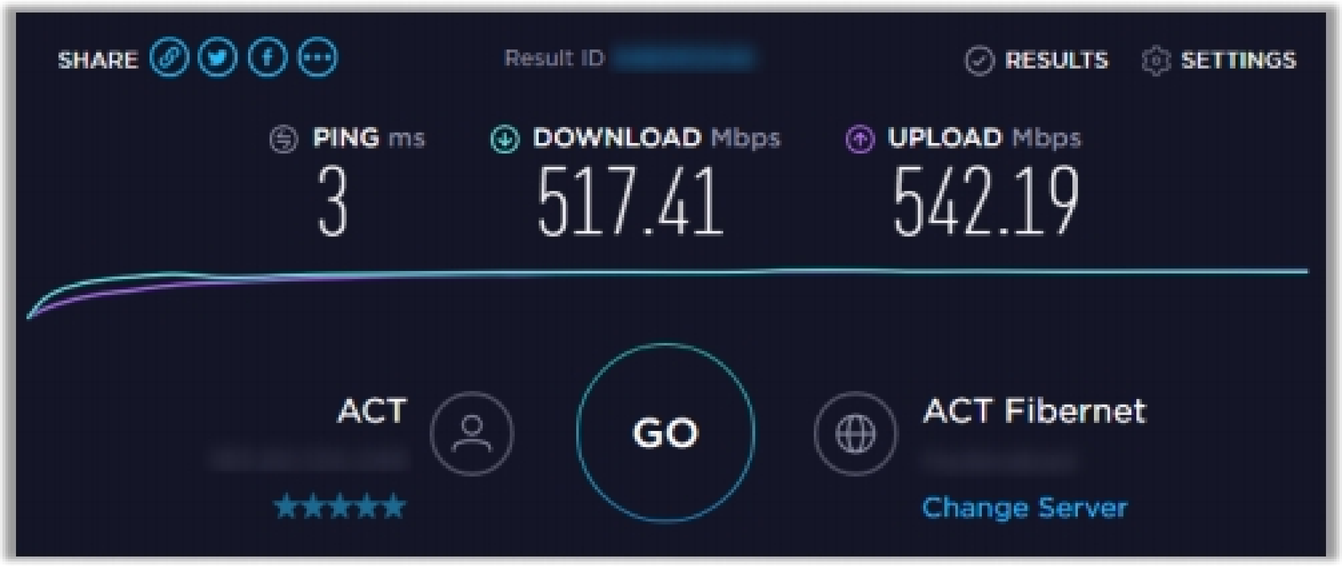
http://downloads.solarwinds.com/solarwinds/Release/FreeTool/SolarWinds-Subnet-Calculator.zip


Bitcricket IP Calculator
File
Options
Help
bitcricket
Next Generation IPv4/v6 Subnet Calculator
Conversions
Classes
Subnets
CIDR
IPv6
Bitcricket
Ethernet Multicast

Dotted Decimal: 10.10.10.2
Decimal: 168430082
Dotted Hexadecimal: 0a.0a.0a.02
Hexadecimal: 0xa0a0a02
Dotted Binary: 00001010.00001010.00001010.00000010
Binary: 00001010000010100000101000000010

Speedtest.net

- Speedtest.net is a website used to **determine the available bandwidth** for a host at the time of testing
- The service provider's assigned values may differ from the actual values of the bandwidth
- This website can determine the time taken to upload and download a file


SHARE
RESULTS
SETTINGS
ACT
GO
ACT Fibernet
Change Server

Result ID [redacted]

PING ms: 3
DOWNLOAD Mbps: 517.41
UPLOAD Mbps: 542.19

ACT [redacted]

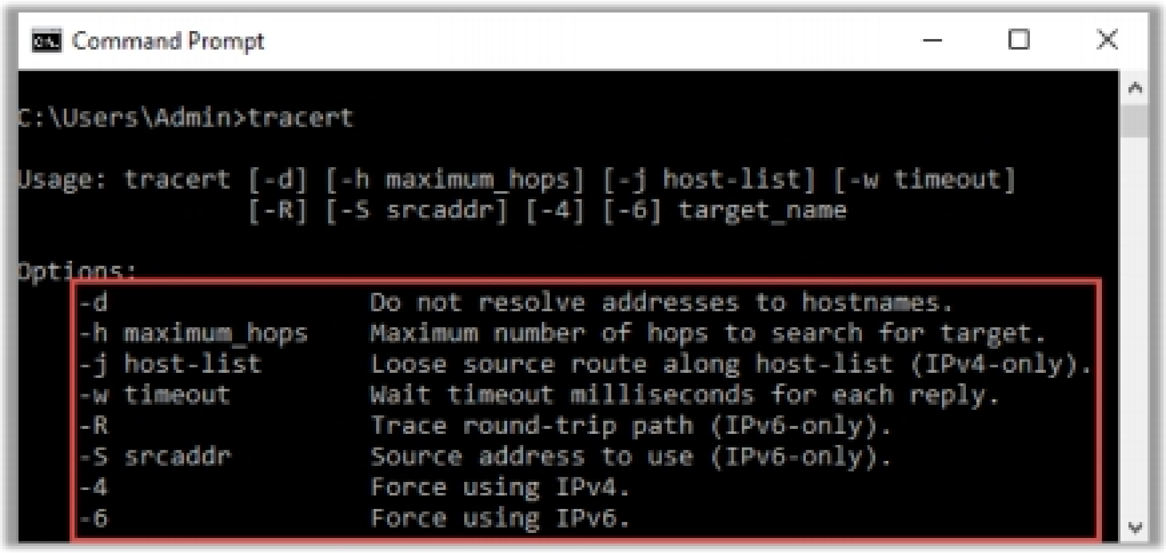
ACT Fibernet [redacted]

Notes: ____

Pathping and mtr

- The **Pathping** utility is used to give detailed information about the **path characteristics** from a specific host to a specific destination in a single picture
- Takes internal advantage of Ping and Traceroute/tracert commands to display the result
- In the first step pathping traces the route to the destination. Then, it runs a 25-second test and collects the rate at which data is lost at each router

- Use the `pathping -n` command to show numeric IP numbers instead of DNS host names

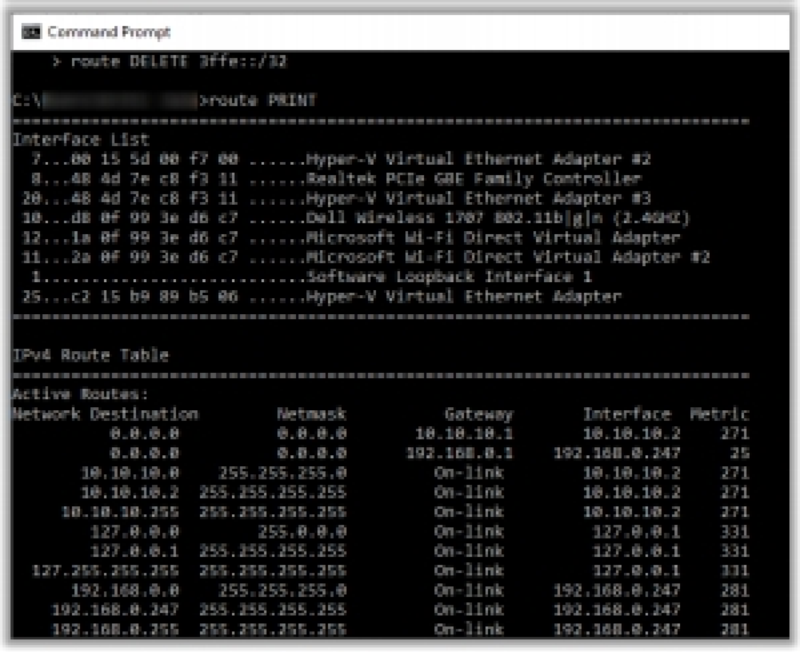


```
C:\Users\Admin>tracert

Usage: tracert [-d] [-h maximum_hops] [-j host-list] [-w timeout]
               [-R] [-S srcaddr] [-4] [-6] target_name

Options:
    -d                 Do not resolve addresses to hostnames.
    -h maximum_hops    Maximum number of hops to search for target.
    -j host-list       Loose source route along host-list (IPv4-only).
    -w timeout         Wait timeout milliseconds for each reply.
    -R                 Trace round-trip path (IPv6-only).
    -S srcaddr         Source address to use (IPv6-only).
    -4                 Force using IPv4.
    -6                 Force using IPv6.
```

Route

- The **Route** utility is used to show the ongoing status of the routing table on the host
- It is more useful when the host has multiple IPs and multiple hosts
- The netmask, network destination, and gateways are displayed in the Active routes section of the Route utility

- `route [-p] command dest [mask subnet] gateway [-if interface]` is the command for adding deleting or changing a route entry



```
    > route DELETE 3ffe::/32

C:\[redacted]>route PRINT
===========================================================================
Interface List
  7...00 15 5d 00 f7 00 ......Hyper-V Virtual Ethernet Adapter #2
  8...48 4d 7e c8 f3 11 ......Realtek PCIe GBE Family Controller
 20...48 4d 7e c8 f3 11 ......Hyper-V Virtual Ethernet Adapter #3
 10...d8 0f 99 3e d6 c7 ......Dell Wireless 1707 802.11b|g|n (2.4GHZ)
 12...1a 0f 99 3e d6 c7 ......Microsoft Wi-Fi Direct Virtual Adapter
 11...2a 0f 99 3e d6 c7 ......Microsoft Wi-Fi Direct Virtual Adapter #2
  1...........................Software Loopback Interface 1
 25...c2 15 b9 89 b5 06 ......Hyper-V Virtual Ethernet Adapter
===========================================================================

IPv4 Route Table
===========================================================================
Active Routes:
Network Destination        Netmask          Gateway       Interface  Metric
          0.0.0.0          0.0.0.0       10.10.10.1      10.10.10.2    271
          0.0.0.0          0.0.0.0      192.168.0.1   192.168.0.247     25
       10.10.10.0    255.255.255.0         On-link       10.10.10.2    271
       10.10.10.2  255.255.255.255         On-link       10.10.10.2    271
     10.10.10.255  255.255.255.255         On-link       10.10.10.2    271
        127.0.0.0        255.0.0.0         On-link        127.0.0.1    331
        127.0.0.1  255.255.255.255         On-link        127.0.0.1    331
  127.255.255.255  255.255.255.255         On-link        127.0.0.1    331
      192.168.0.0    255.255.255.0         On-link    192.168.0.247    281
    192.168.0.247  255.255.255.255         On-link    192.168.0.247    281
    192.168.0.255  255.255.255.255         On-link    192.168.0.247    281
```

Notes: ____

____

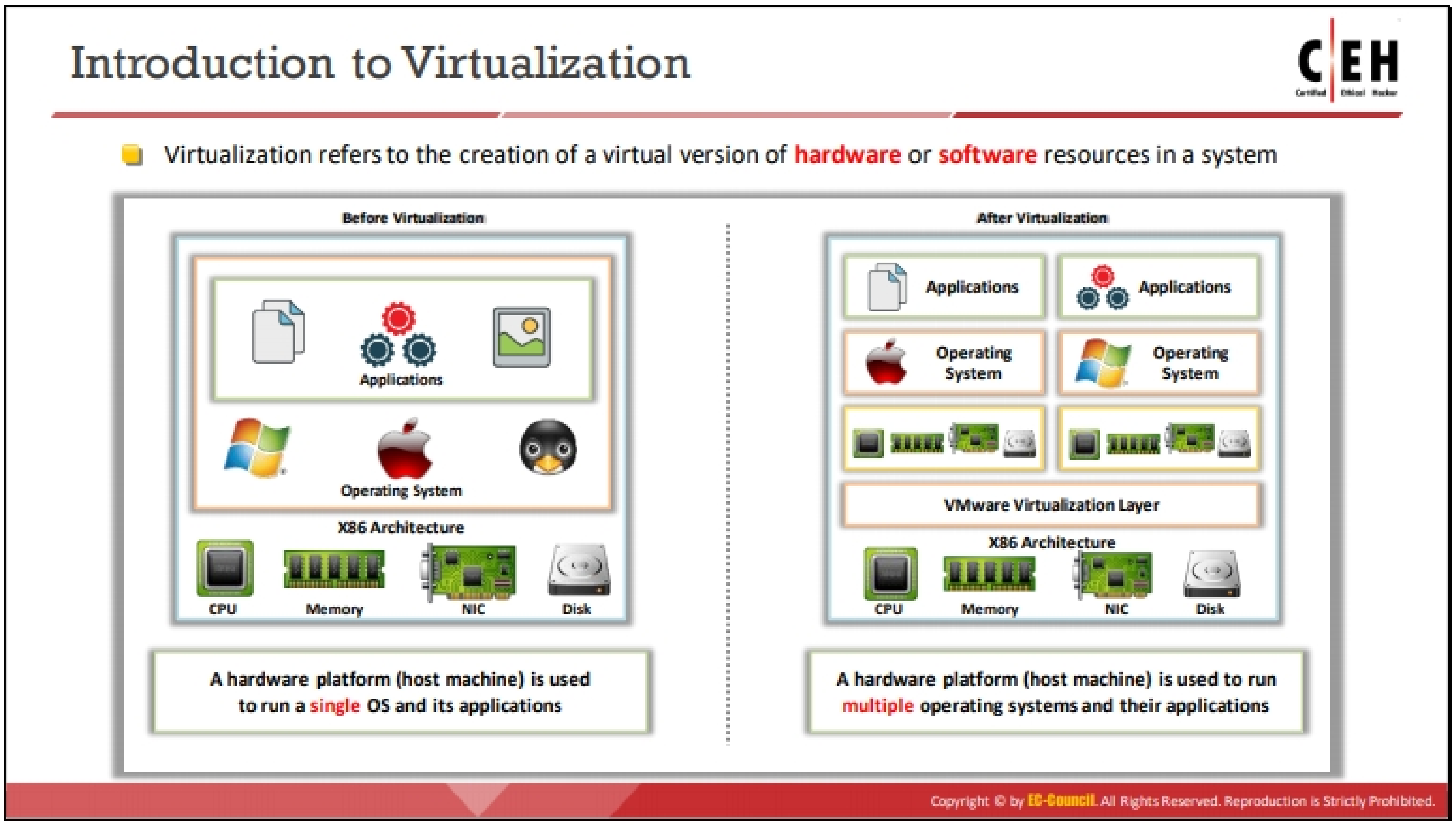
____

____

____

____

Virtualization



Introduction to Virtualization

- Virtualization refers to the creation of a virtual version of **hardware** or **software** resources in a system

Before Virtualization

Applications
Operating System
X86 Architecture
CPU
Memory
NIC
Disk

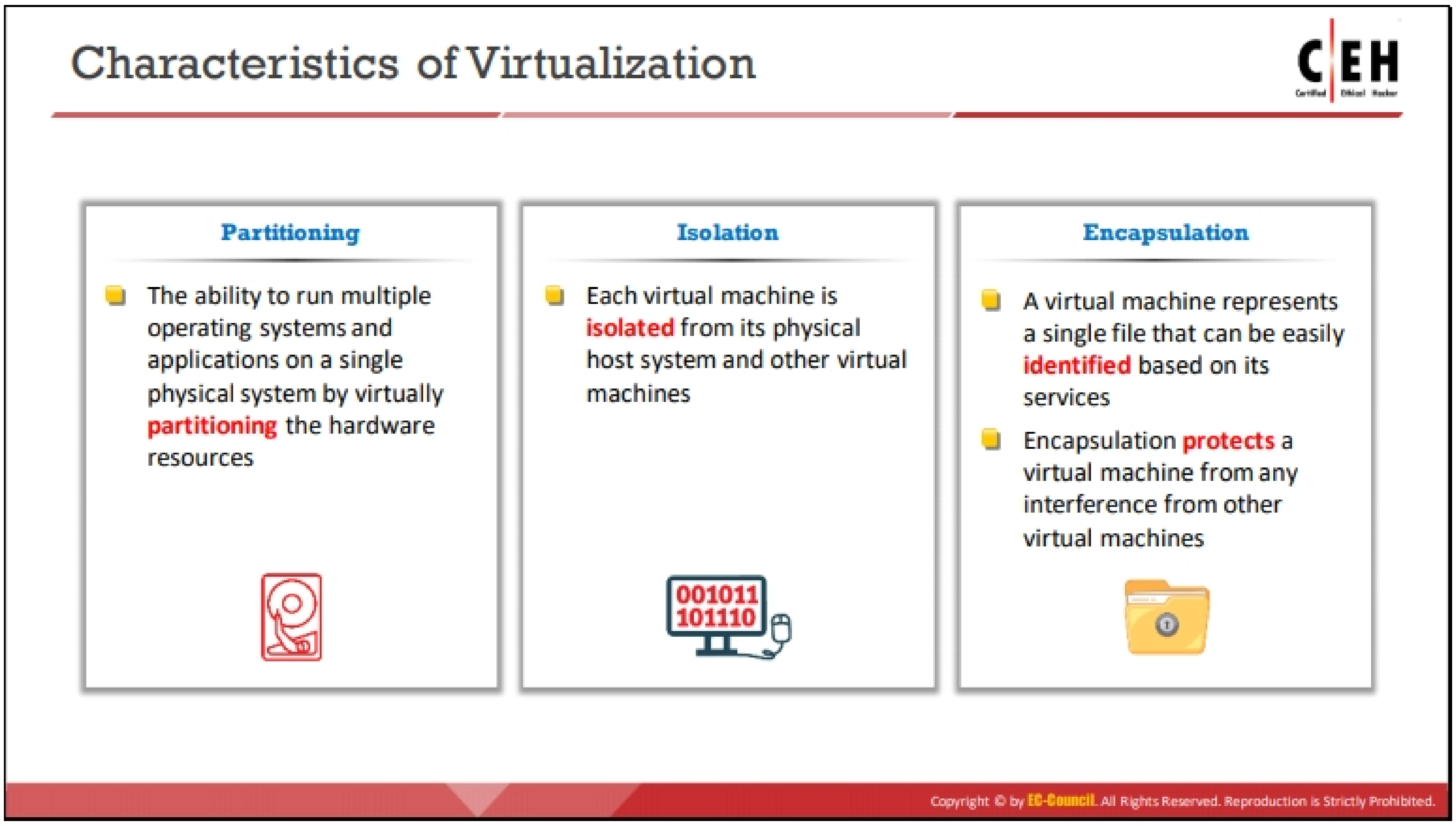
A hardware platform (host machine) is used to run a single OS and its applications

After Virtualization

Applications
Applications
Operating System
Operating System
VMware Virtualization Layer
X86 Architecture
CPU
Memory
NIC
Disk

A hardware platform (host machine) is used to run multiple operating systems and their applications

Notes:



Characteristics of Virtualization

Partitioning

- The ability to run multiple operating systems and applications on a single physical system by virtually **partitioning** the hardware resources

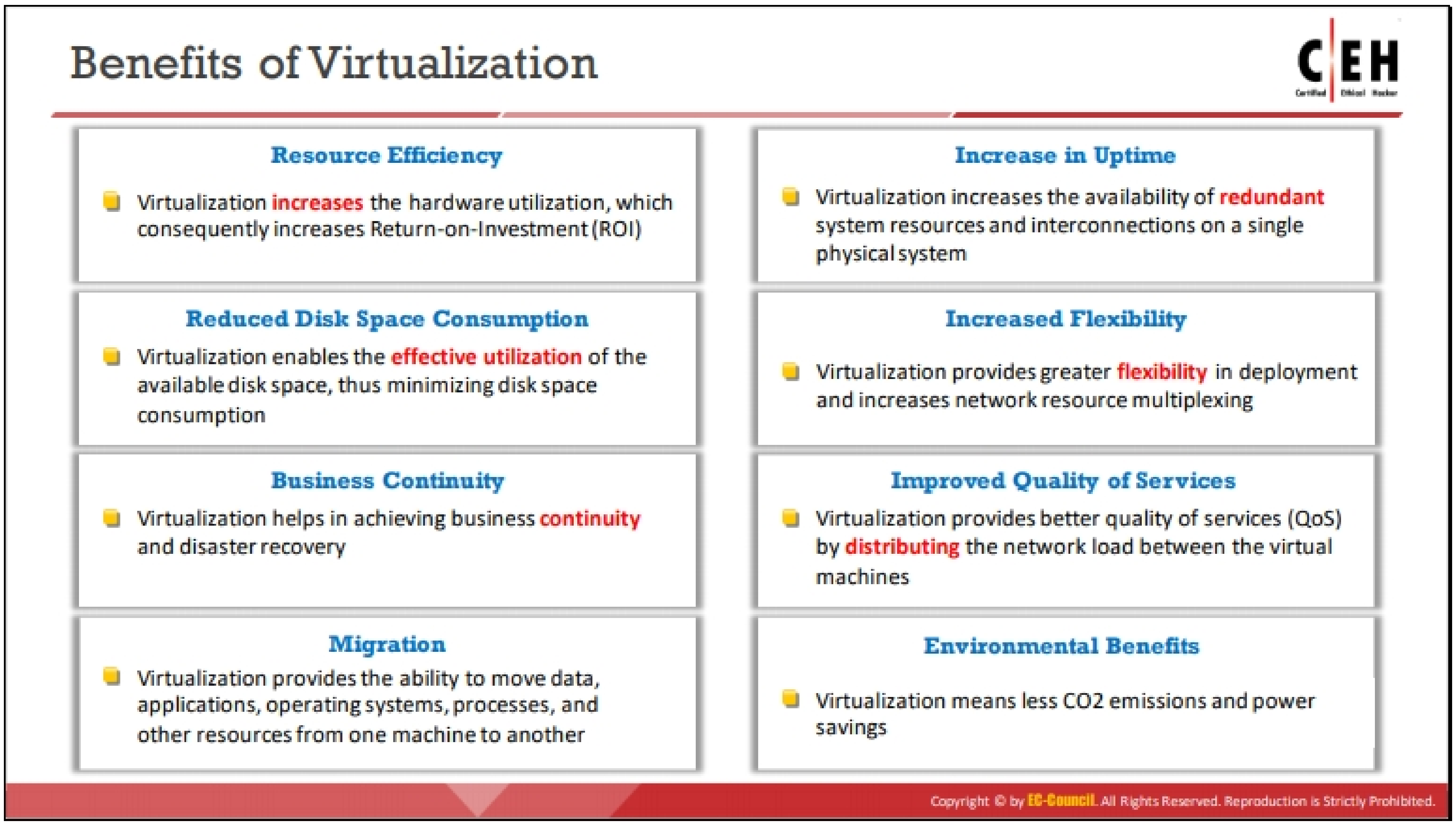
Isolation

- Each virtual machine is **isolated** from its physical host system and other virtual machines

001011
101110

Encapsulation

- A virtual machine represents a single file that can be easily **identified** based on its services
- Encapsulation **protects** a virtual machine from any interference from other virtual machines



Benefits of Virtualization

Resource Efficiency

- Virtualization **increases** the hardware utilization, which consequently increases Return-on-Investment (ROI)

Increase in Uptime

- Virtualization increases the availability of **redundant** system resources and interconnections on a single physical system

Reduced Disk Space Consumption

- Virtualization enables the **effective utilization** of the available disk space, thus minimizing disk space consumption

Increased Flexibility

- Virtualization provides greater **flexibility** in deployment and increases network resource multiplexing

Business Continuity

- Virtualization helps in achieving business **continuity** and disaster recovery

Improved Quality of Services

- Virtualization provides better quality of services (QoS) by **distributing** the network load between the virtual machines

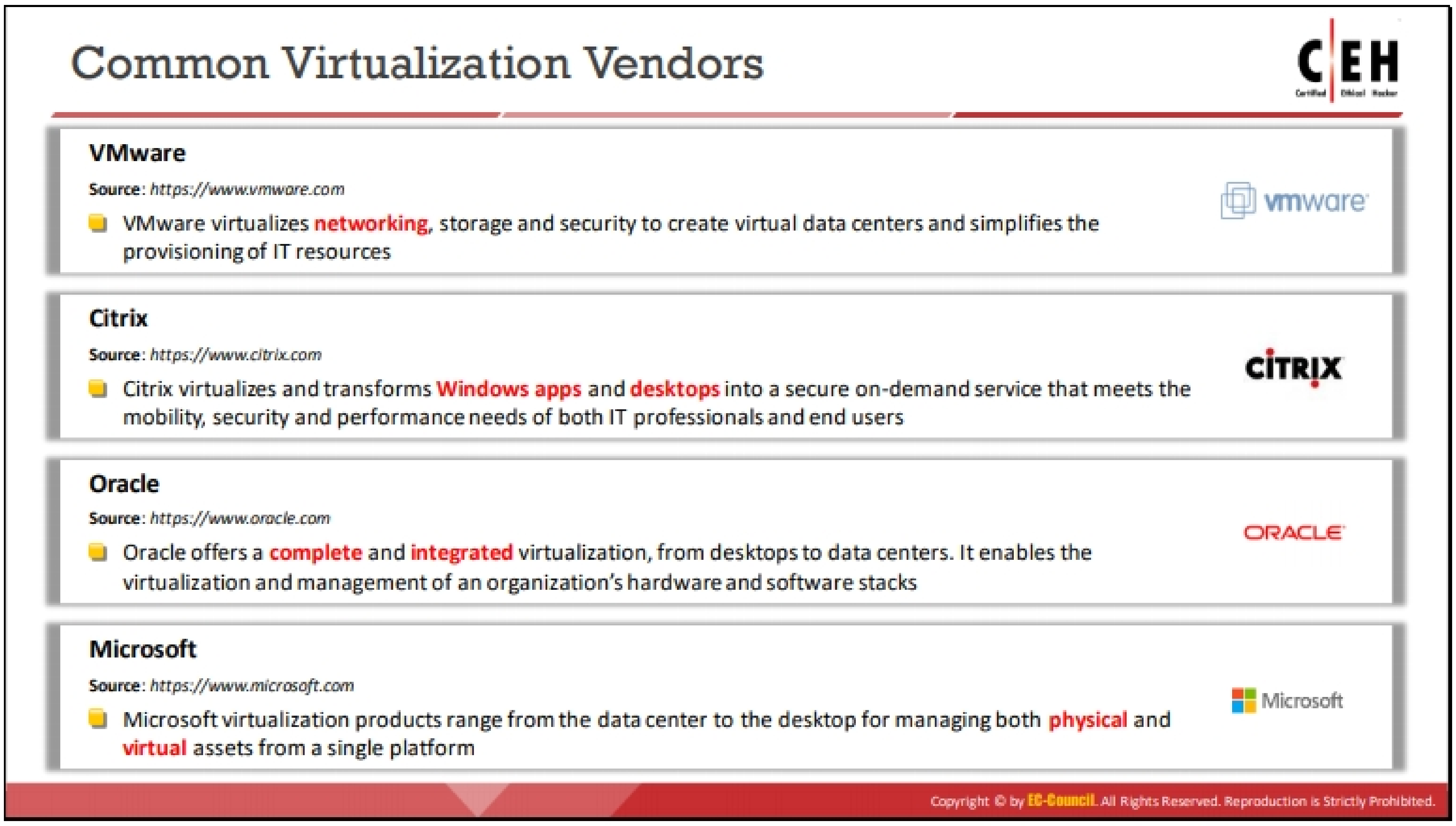
Migration

- Virtualization provides the ability to move data, applications, operating systems, processes, and other resources from one machine to another

Environmental Benefits

- Virtualization means less CO2 emissions and power savings

Notes:



Common Virtualization Vendors

VMware

Source: *https://www.vmware.com*

- VMware virtualizes **networking**, storage and security to create virtual data centers and simplifies the provisioning of IT resources

Citrix

Source: *https://www.citrix.com*

- Citrix virtualizes and transforms **Windows apps** and **desktops** into a secure on-demand service that meets the mobility, security and performance needs of both IT professionals and end users

Oracle

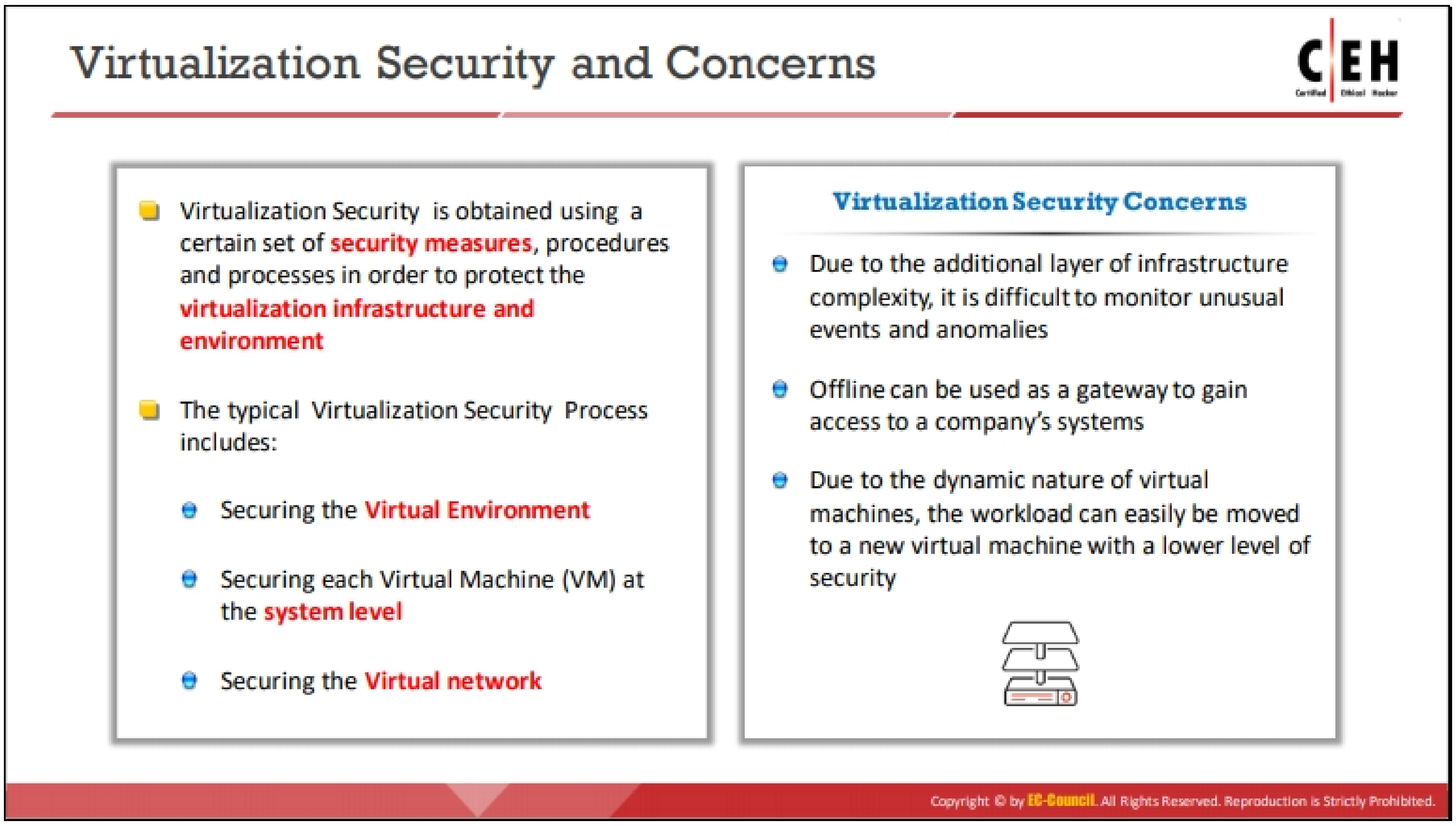
Source: *https://www.oracle.com*

- Oracle offers a **complete** and **integrated** virtualization, from desktops to data centers. It enables the virtualization and management of an organization's hardware and software stacks

Microsoft

Source: *https://www.microsoft.com*

- Microsoft virtualization products range from the data center to the desktop for managing both **physical** and **virtual** assets from a single platform



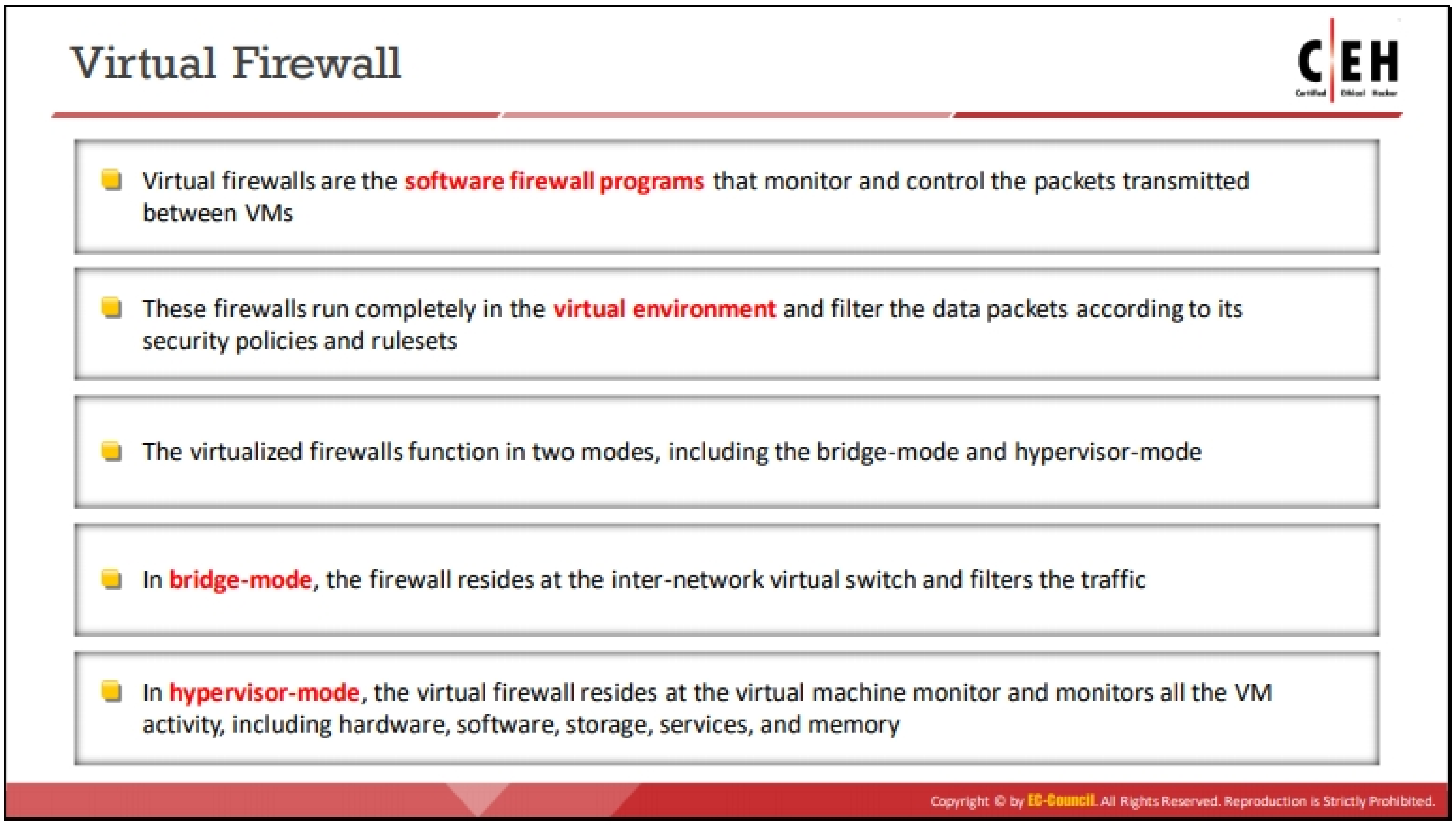
Virtualization Security and Concerns

- Virtualization Security is obtained using a certain set of **security measures**, procedures and processes in order to protect the **virtualization infrastructure and environment**
- The typical Virtualization Security Process includes:
  - Securing the **Virtual Environment**
  - Securing each Virtual Machine (VM) at the **system level**
  - Securing the **Virtual network**

Virtualization Security Concerns

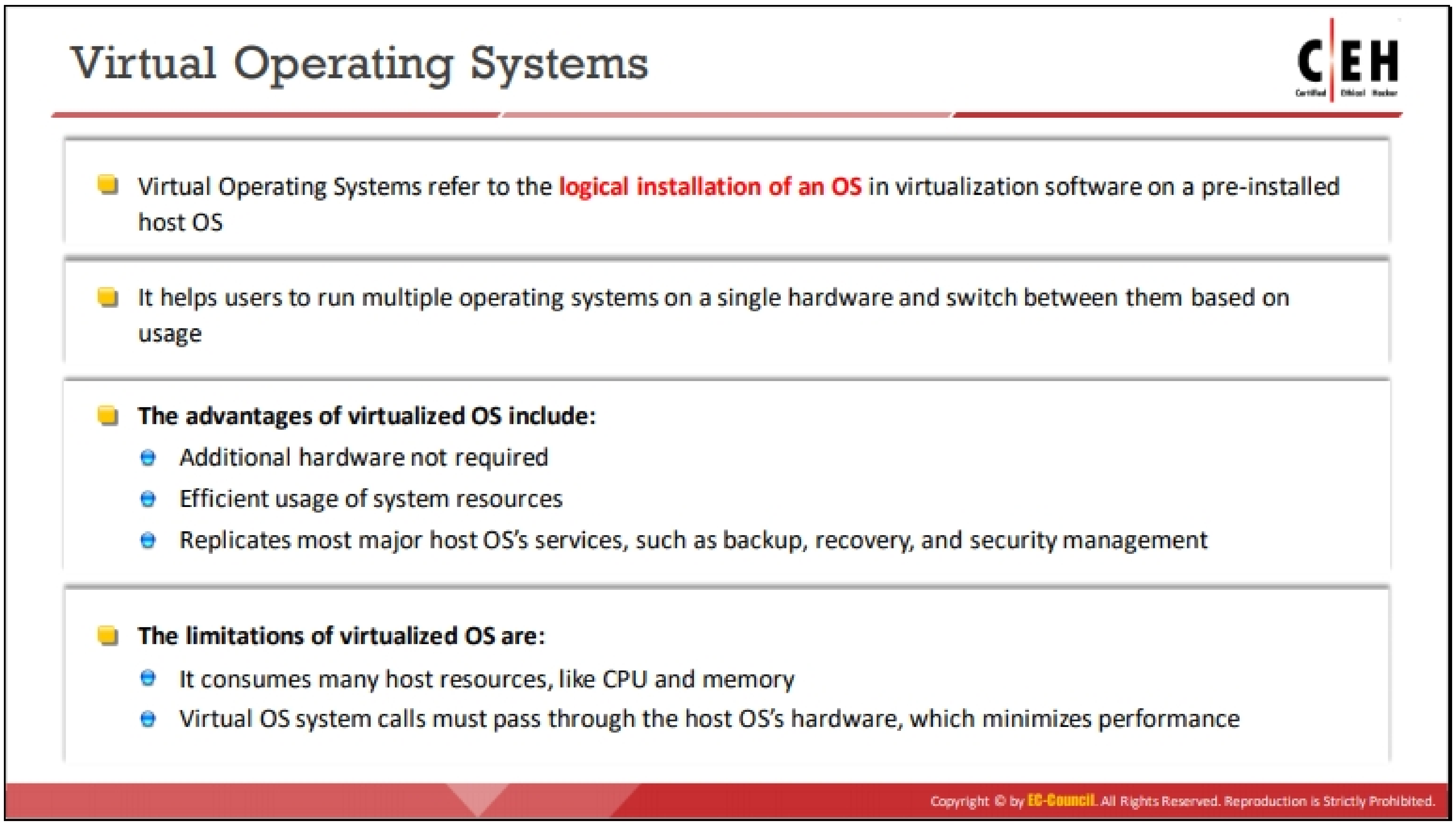
- Due to the additional layer of infrastructure complexity, it is difficult to monitor unusual events and anomalies
- Offline can be used as a gateway to gain access to a company's systems
- Due to the dynamic nature of virtual machines, the workload can easily be moved to a new virtual machine with a lower level of security

Notes:



Virtual Firewall

- Virtual firewalls are the **software firewall programs** that monitor and control the packets transmitted between VMs
- These firewalls run completely in the **virtual environment** and filter the data packets according to its security policies and rulesets
- The virtualized firewalls function in two modes, including the bridge-mode and hypervisor-mode
- In **bridge-mode**, the firewall resides at the inter-network virtual switch and filters the traffic
- In **hypervisor-mode**, the virtual firewall resides at the virtual machine monitor and monitors all the VM activity, including hardware, software, storage, services, and memory



Virtual Operating Systems

- Virtual Operating Systems refer to the **logical installation of an OS** in virtualization software on a pre-installed host OS
- It helps users to run multiple operating systems on a single hardware and switch between them based on usage
- **The advantages of virtualized OS include:**
  - Additional hardware not required
  - Efficient usage of system resources
  - Replicates most major host OS's services, such as backup, recovery, and security management
- **The limitations of virtualized OS are:**
  - It consumes many host resources, like CPU and memory
  - Virtual OS system calls must pass through the host OS's hardware, which minimizes performance

Notes: ____

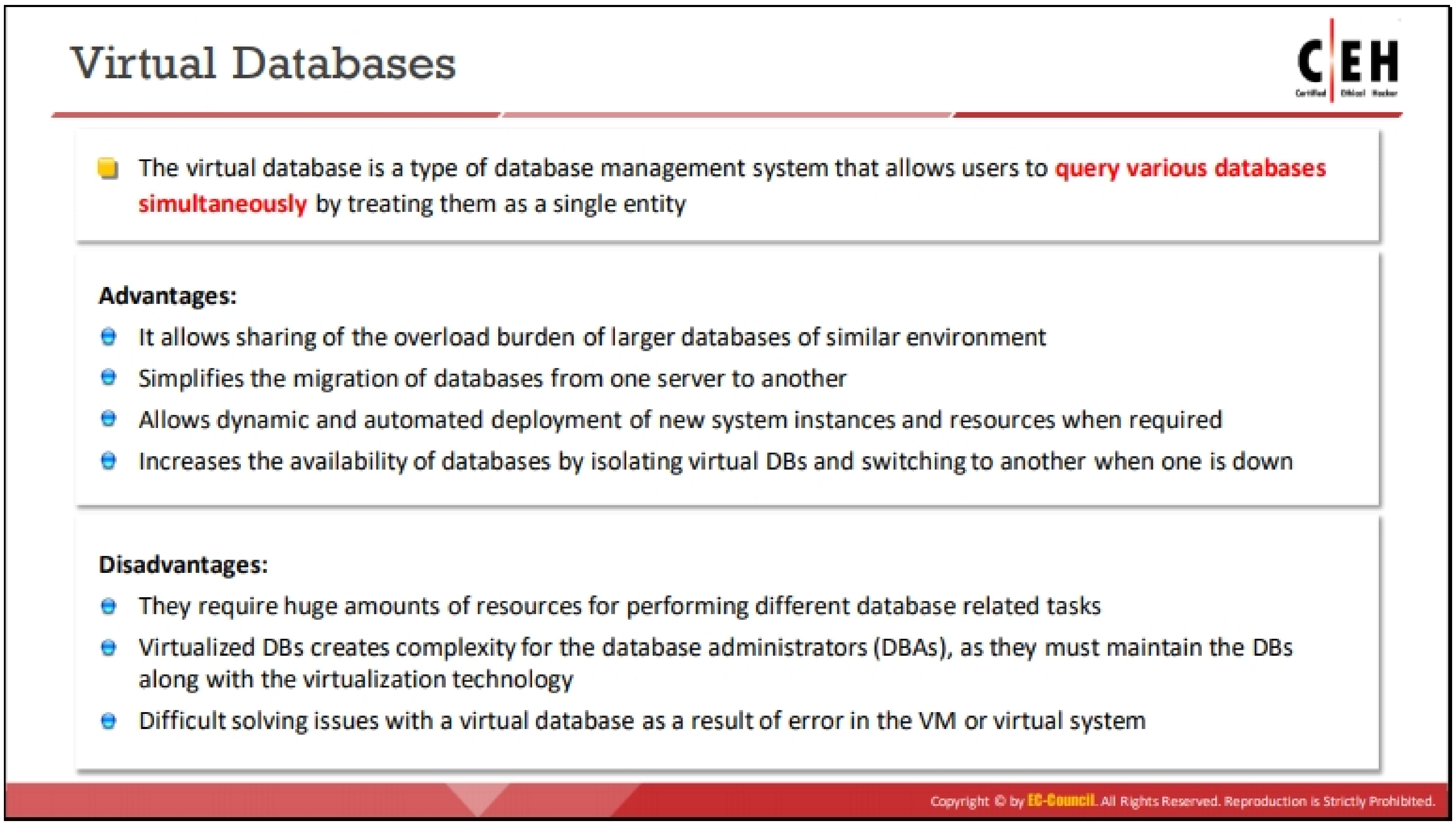
____

____

____

____

____



Virtual Databases

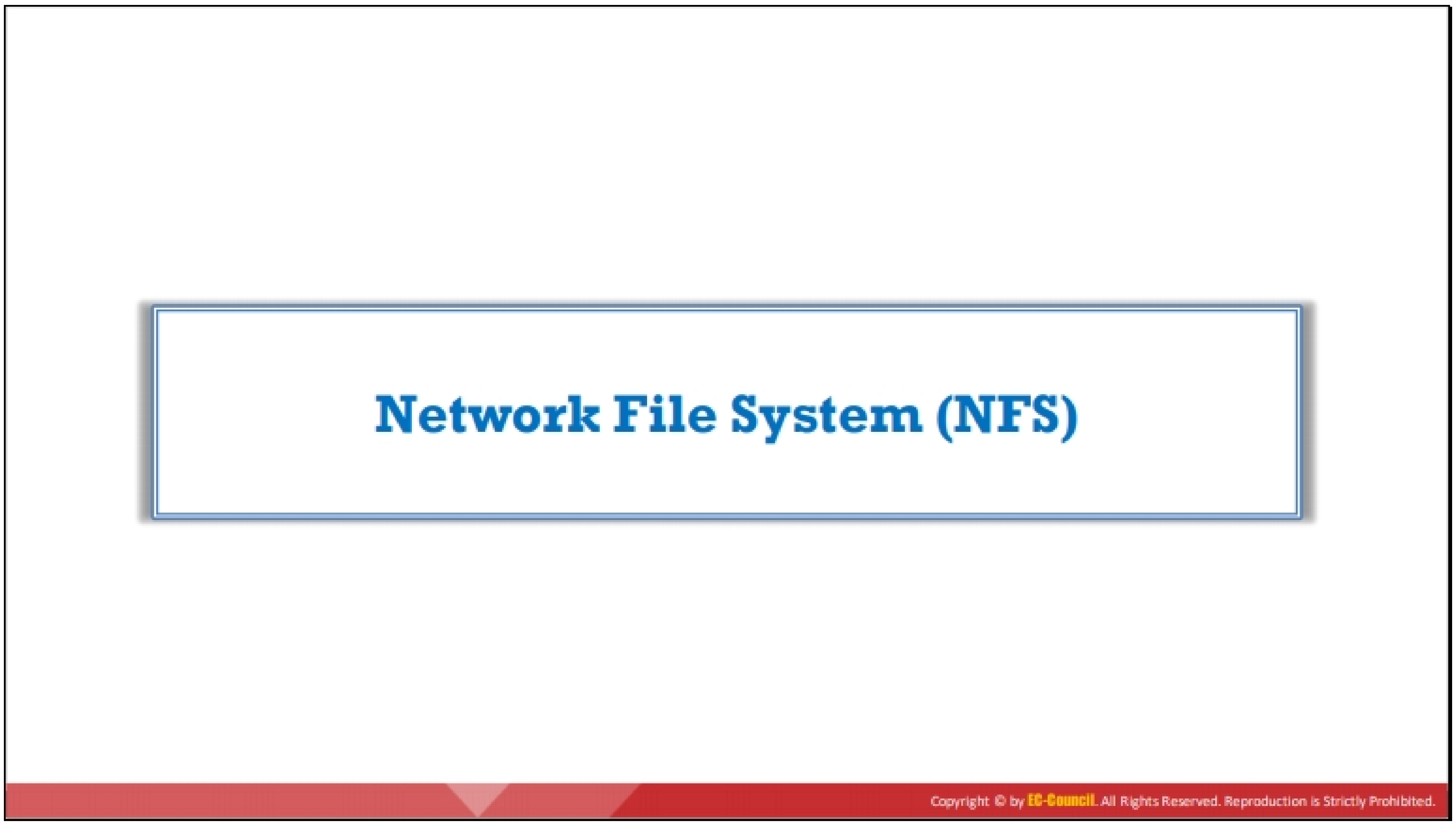
- The virtual database is a type of database management system that allows users to **query various databases simultaneously** by treating them as a single entity

Advantages:

- It allows sharing of the overload burden of larger databases of similar environment
- Simplifies the migration of databases from one server to another
- Allows dynamic and automated deployment of new system instances and resources when required
- Increases the availability of databases by isolating virtual DBs and switching to another when one is down

Disadvantages:

- They require huge amounts of resources for performing different database related tasks
- Virtualized DBs creates complexity for the database administrators (DBAs), as they must maintain the DBs along with the virtualization technology
- Difficult solving issues with a virtual database as a result of error in the VM or virtual system



Network File System (NFS)

Notes:

Network File System (NFS)

- The Network File System (NFS) is a **distributed file system protocol** that allows users to read, write, store, and access files across devices connected through a network
- The file system works on all **IP-based networks** and uses TCP\UDP for data access and delivery

NFS Security

- NFS offers the following two types of security:
  - Host level (access control)
  - File level (operational)

NFS Host and File Level Security

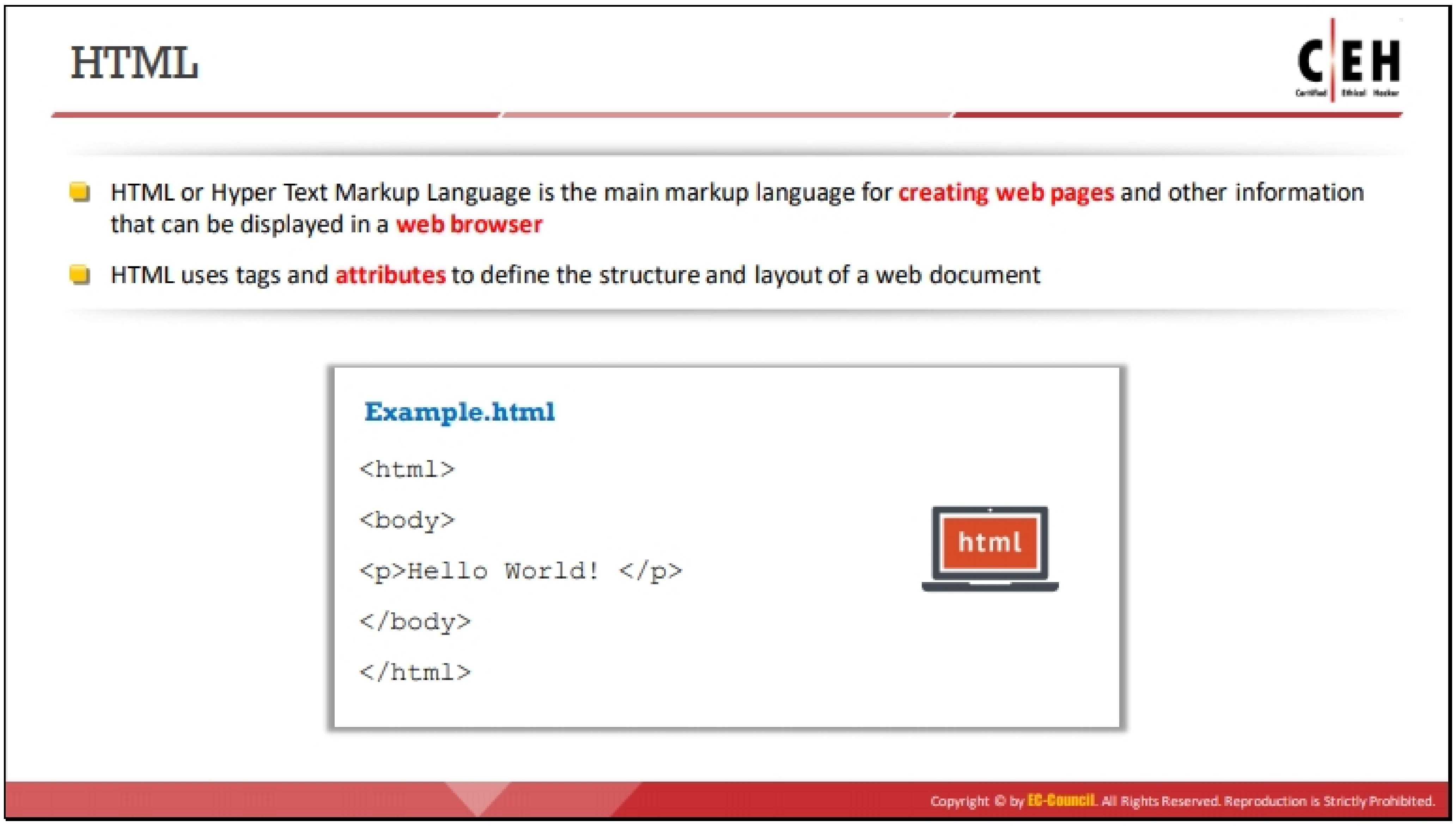
- Host level security refers to **restricting certain operations** when the remote user does not provide correct credentials
- File level security refers to limiting actions on the files in a mounted file system

Methods of securing access controls in NFS include:

Root squashing	nosuid	noexec
The process of limiting superuser access privileges using identity authentication To enforce restrictions on the superuser, the administrators map the root's UID to the anonymous user in the NFS RPC credential structure	Does not allow the SUID or SGID to take effect on this filesystem Uses the nosuid option to prevent the execution of NFS mounted user identity executables on the host	Prevents the execution of files from this partition Uses the noexec option to prevent a user's identity from executing binaries

Notes: ______________________________

Web Markup and Programming Languages



HTML

- HTML or Hyper Text Markup Language is the main markup language for **creating web pages** and other information that can be displayed in a **web browser**
- HTML uses tags and **attributes** to define the structure and layout of a web document

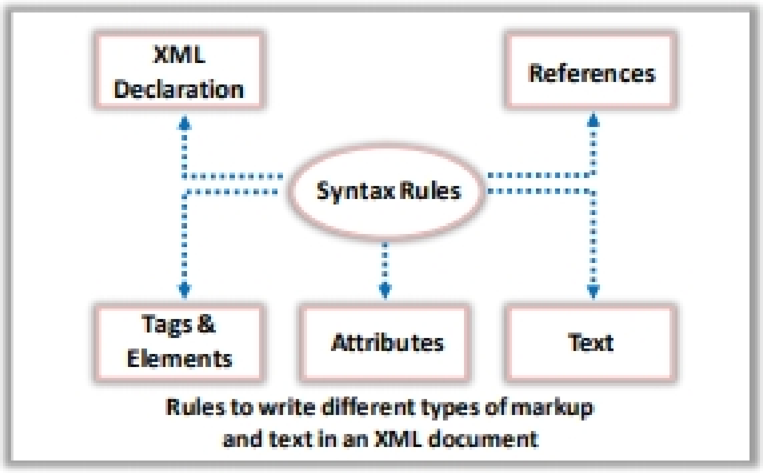
Example.html

```
<html>
<body>
<p>Hello World! </p>
</body>
</html>
```

Notes:

Extensible Markup Language (XML)

- XML is a markup language that defines a certain **set of rules for converting data** in a machine- and human-readable format
- It is derived from the **Standard Generalized Markup Language** (SGML)
- It is designed to store and transport data



XML Declaration
References
Syntax Rules
Tags & Elements
Attributes
Text

Rules to write different types of markup and text in an XML document

Characteristics

- Extensible
- Carries, but does not present, the data
- A public standard

Advantages

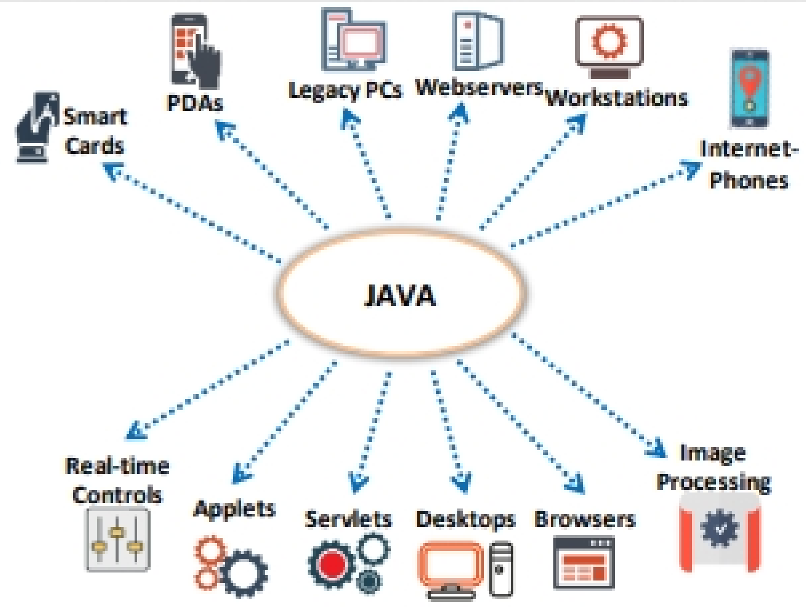
- Used to exchange information between organizations and systems
- Used for offloading and reloading databases
- Used to store and arrange data, which can customize your data handling needs
- Easily merges with style sheets to create almost any desired output

Java

- Java is an **object-oriented** application programming language developed by **Sun Microsystems** and designed for use in **distributed** environments
- It can be used to build a small application **module**, or **applet**, for use as part of a web page
- Java supports a large set of **protocols**, **mechanisms**, **tools**, **API's**, **security algorithms**, and other resources that help in securing the application code

Features

- Platform-independent
- Multithreaded programming
- Built-in support for computer networks
- Automatic garbage collection
- Designed to securely execute code from remote sources
- Designed to handle exceptions
- Portability



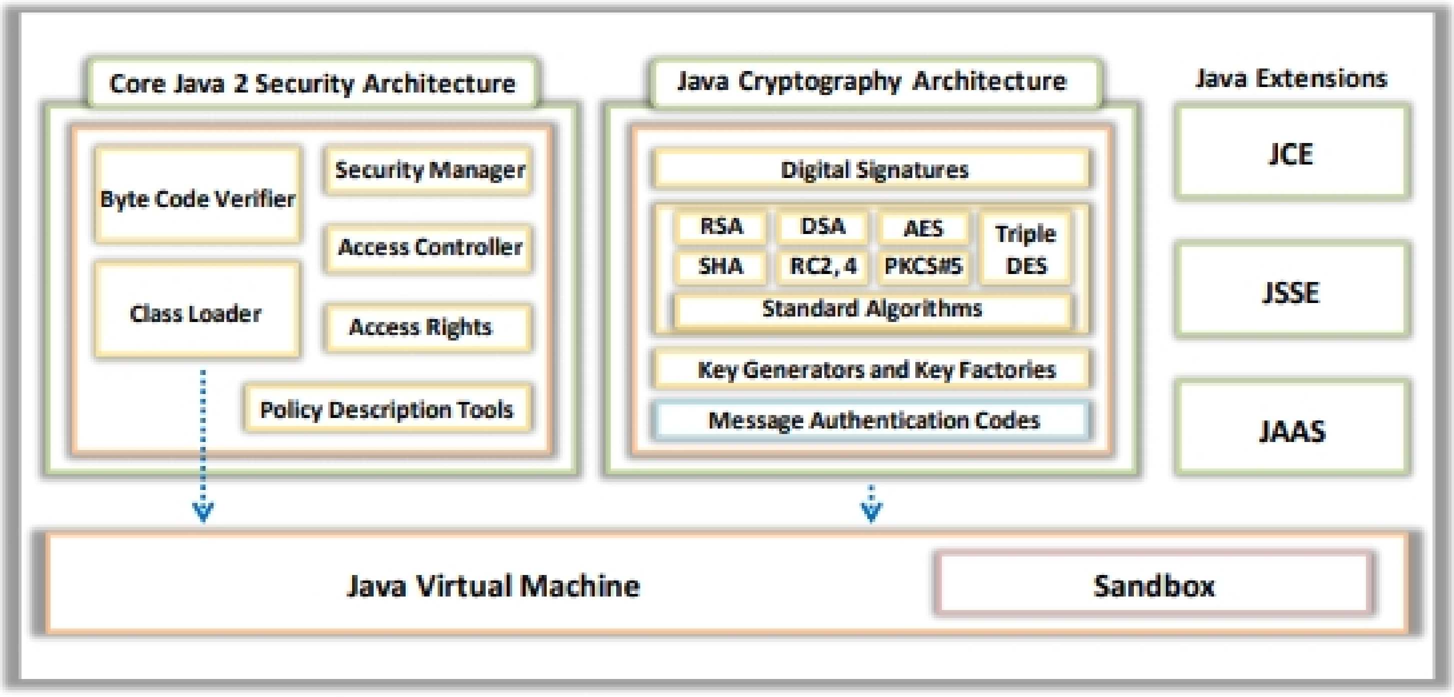
JAVA
Smart Cards
PDAs
Legacy PCs
Webservers
Workstations
Internet-Phones
Real-time Controls
Applets
Servlets
Desktops
Browsers
Image Processing

Notes: ____

Java (Cont'd)

Java Security Platform

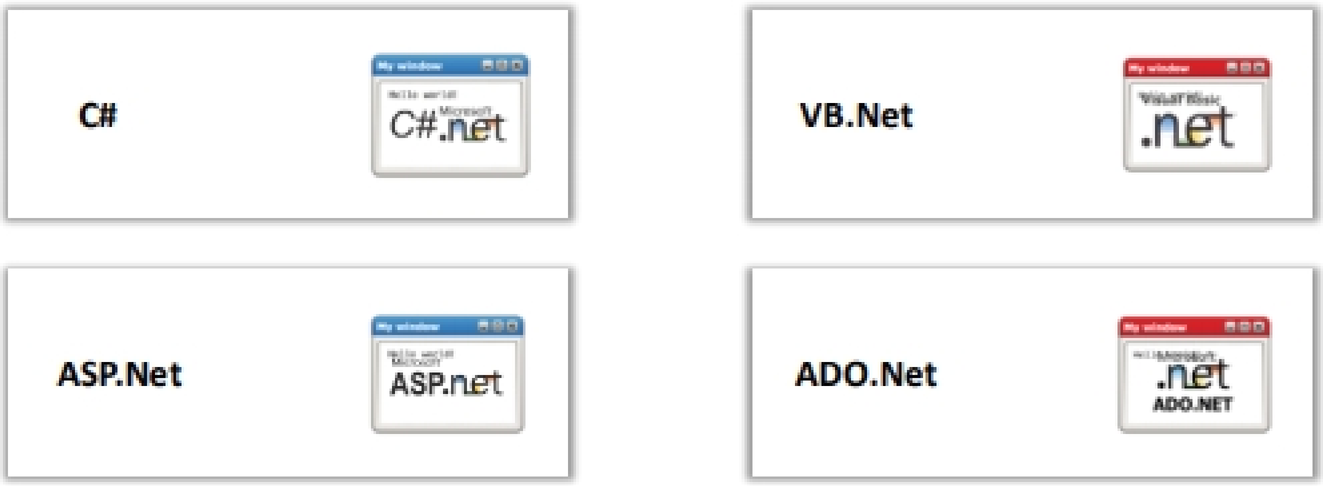
- The Java security platform is formed by two parts: **Core Java Security Architecture** and **Java Cryptography Architecture**


Core Java 2 Security Architecture
Byte Code Verifier
Security Manager
Access Controller
Class Loader
Access Rights
Policy Description Tools
Java Cryptography Architecture
Digital Signatures
RSA
DSA
AES
Triple DES
SHA
RC2, 4
PKCS#5
Standard Algorithms
Key Generators and Key Factories
Message Authentication Codes
Java Extensions
JCE
JSSE
JAAS
Java Virtual Machine
Sandbox

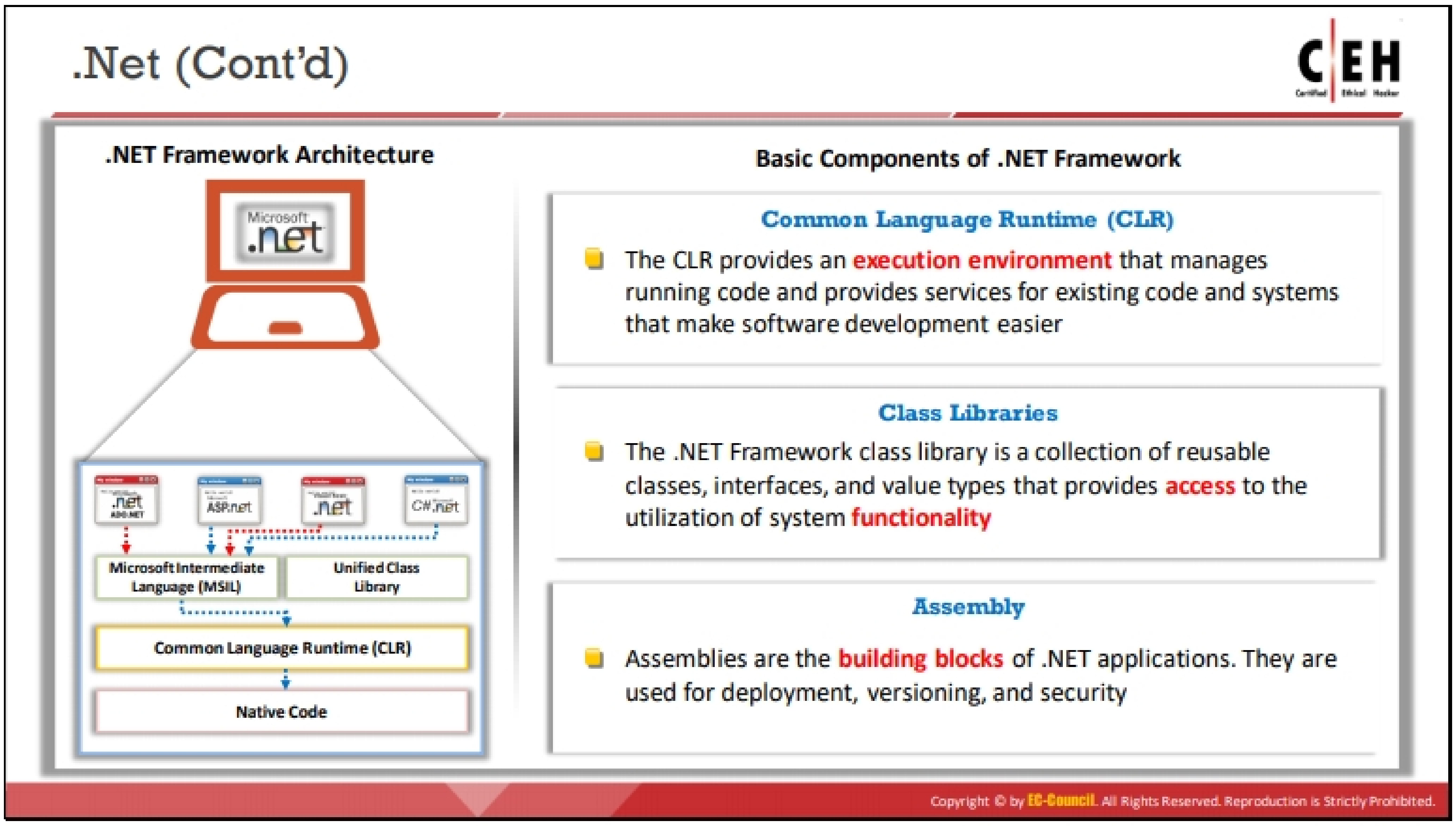
.Net

- Microsoft .NET is Microsoft's **software programming** architecture that creates Internet-enabled and web-based applications
- It consists of **several technologies** that allow software developers to build Internet-based distributed systems

.NET implementation includes the following


C#
VB.Net
ASP.Net
ADO.Net
C#.net
.net
ASP.net
.net
ADO.NET

Notes: ____________________



.Net (Cont'd)

.NET Framework Architecture

Basic Components of .NET Framework

Common Language Runtime (CLR)

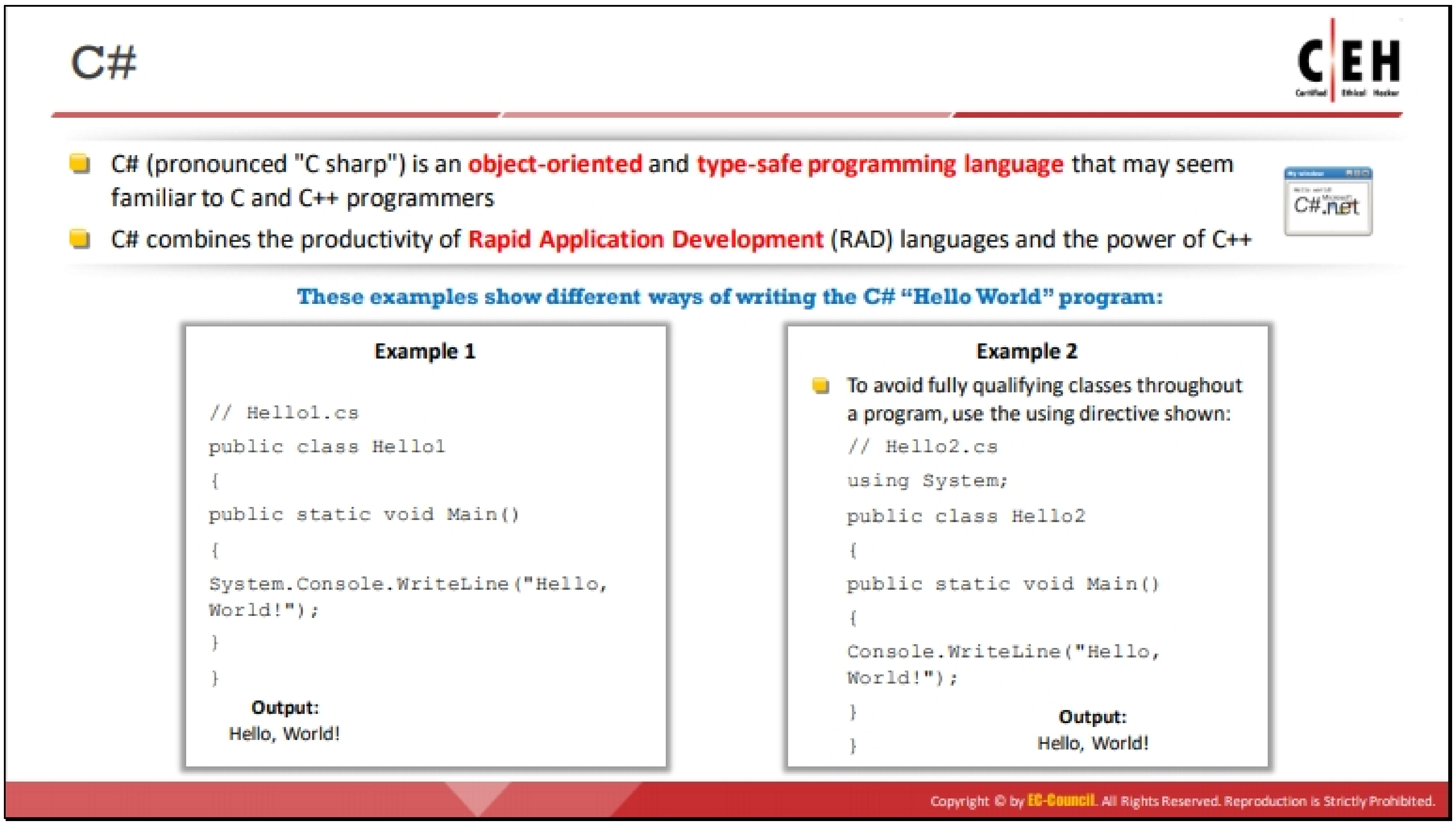
- The CLR provides an **execution environment** that manages running code and provides services for existing code and systems that make software development easier

Class Libraries

- The .NET Framework class library is a collection of reusable classes, interfaces, and value types that provides **access** to the utilization of system **functionality**

Assembly

- Assemblies are the **building blocks** of .NET applications. They are used for deployment, versioning, and security



C#

- C# (pronounced "C sharp") is an **object-oriented** and **type-safe programming language** that may seem familiar to C and C++ programmers
- C# combines the productivity of **Rapid Application Development** (RAD) languages and the power of C++

These examples show different ways of writing the C# "Hello World" program:

Example 1

```
// Hello1.cs
public class Hello1
{
public static void Main()
{
System.Console.WriteLine("Hello,
World!");
}
}
```

Output:

```
Hello, World!
```

Example 2

- To avoid fully qualifying classes throughout a program, use the using directive shown:

```
// Hello2.cs
using System;
public class Hello2
{
public static void Main()
{
Console.WriteLine("Hello,
World!");
}
}
```

Output:

```
Hello, World!
```

Notes: ____

____

____

____

____

____

Java Server Pages (JSP)

- JSP is a Java-based technology that helps you **develop dynamic web pages**
- It runs in a server-side component known as a **JSP container**
- It is similar to ASP and PHP, but it uses the java programing language

Fundamental Tags

- <%....%> Scriptlets
- <%!....%> Declarative
- %@....% Directive
- <%=...%> Expression

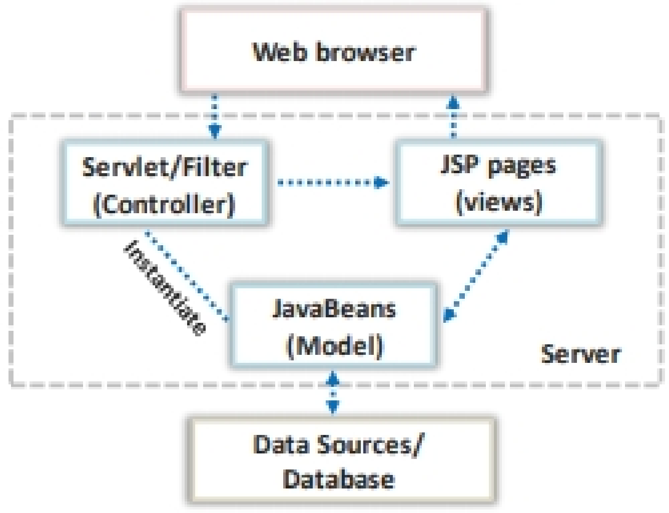
Advantages

- Supports HTML and Java code
- Supports standard web development tools
- Easy language and tags

Disadvantages

- Difficult to debug because JSP pages are converted into servlets and then compiled
- Database connectivity is not as easy as expected
- Extremely difficult to choose the appropriate servlet engine

The JSP Model 2 architecture


Web browser
Servlet/Filter (Controller)
JSP pages (views)
Instantiate
JavaBeans (Model)
Server
Data Sources/ Database

Active Server Pages (ASP)

- ASP is Microsoft's development framework for **building dynamic web pages**

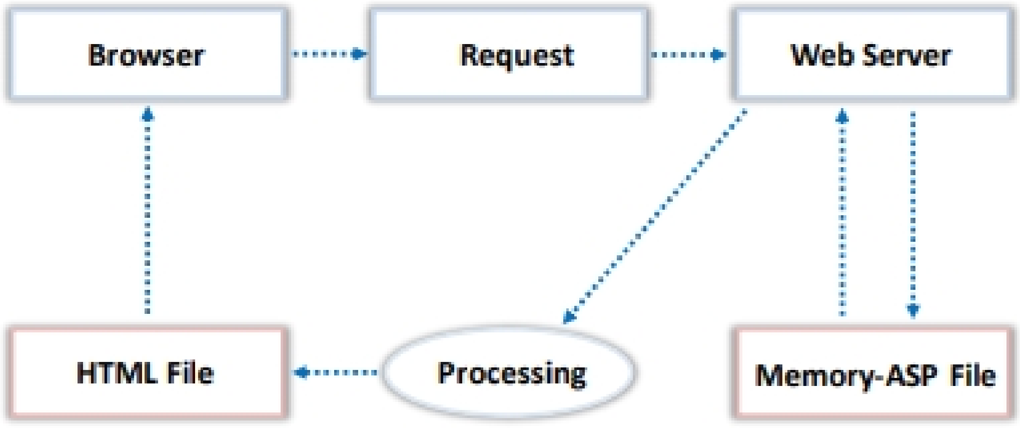
Advantages

- Provides 3-tier architecture
- Compatible with about 55 languages
- Consistent programming model
- Provides direct security support

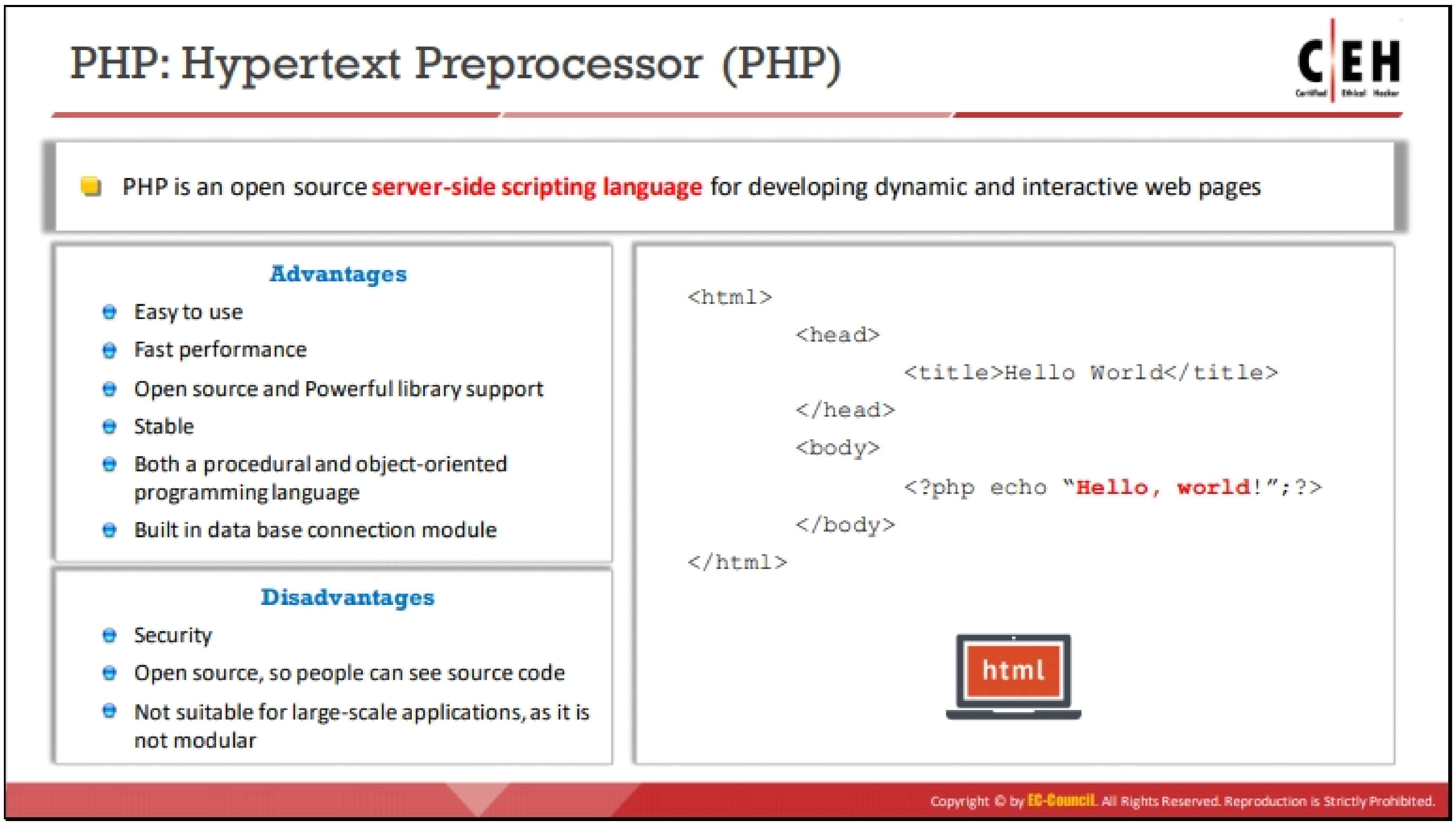
Disadvantages

- Limited ability for client event control
- Interpreted and loosely-typed code
- Mixes layout (HTML) and logic (scripting code)
- Limited development and debugging tools
- No real state management

Processing of an ASP page


Browser
Request
Web Server
HTML File
Processing
Memory-ASP File

Notes: ____



PHP: Hypertext Preprocessor (PHP)

- PHP is an open source **server-side scripting language** for developing dynamic and interactive web pages

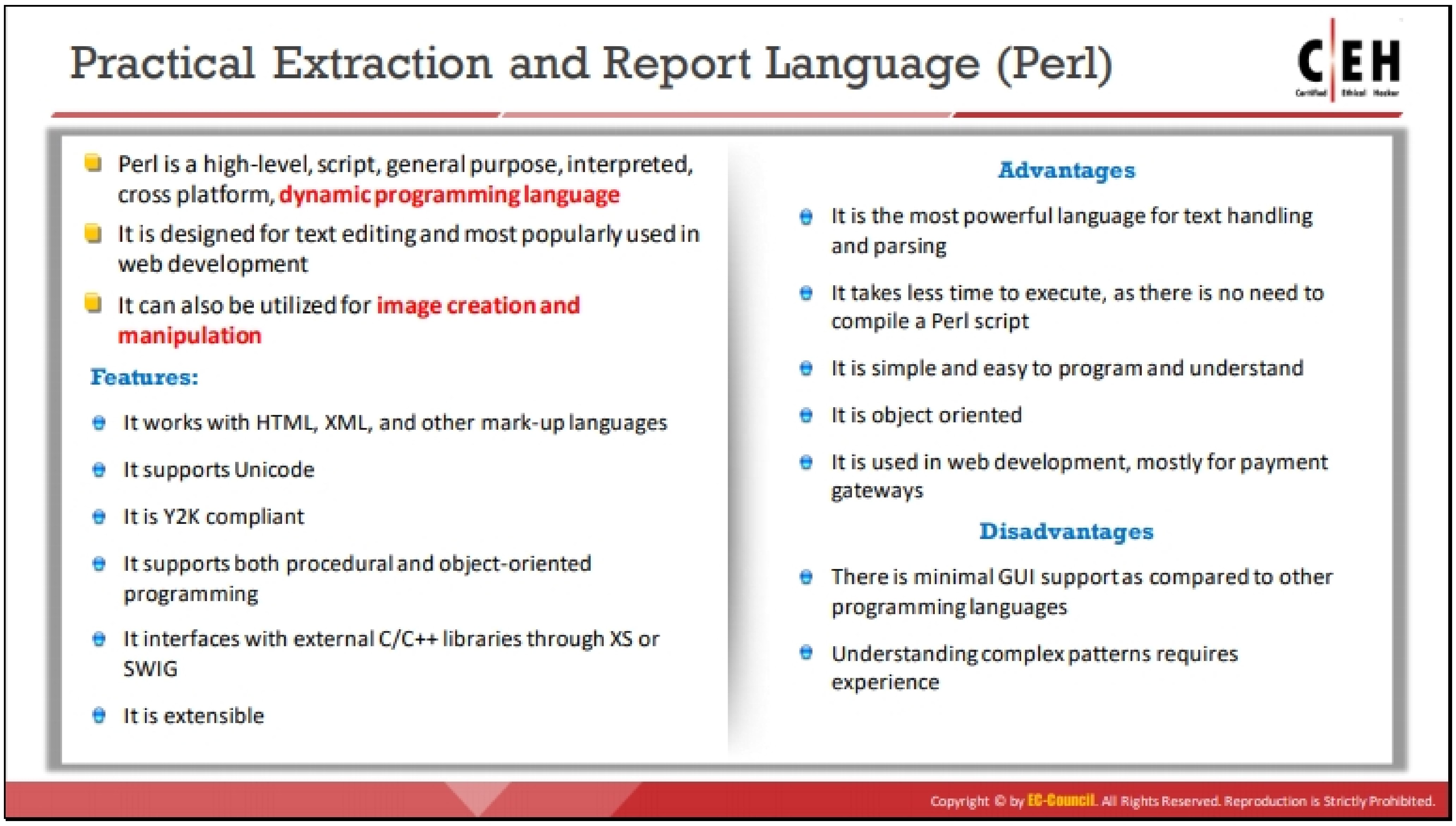
Advantages

- Easy to use
- Fast performance
- Open source and Powerful library support
- Stable
- Both a procedural and object-oriented programming language
- Built in data base connection module

Disadvantages

- Security
- Open source, so people can see source code
- Not suitable for large-scale applications, as it is not modular

```
<html>
       <head>
              <title>Hello World</title>
       </head>
       <body>
              <?php echo "Hello, world!";?>
       </body>
</html>
```



Practical Extraction and Report Language (Perl)

- Perl is a high-level, script, general purpose, interpreted, cross platform, **dynamic programming language**
- It is designed for text editing and most popularly used in web development
- It can also be utilized for **image creation and manipulation**

Features:

- It works with HTML, XML, and other mark-up languages
- It supports Unicode
- It is Y2K compliant
- It supports both procedural and object-oriented programming
- It interfaces with external C/C++ libraries through XS or SWIG
- It is extensible

Advantages

- It is the most powerful language for text handling and parsing
- It takes less time to execute, as there is no need to compile a Perl script
- It is simple and easy to program and understand
- It is object oriented
- It is used in web development, mostly for payment gateways

Disadvantages

- There is minimal GUI support as compared to other programming languages
- Understanding complex patterns requires experience

Notes: ____

JavaScript

- JavaScript is a dynamic computer programming scripting language that **works in all major browsers**, such as Internet Explorer, Mozilla, Firefox, Netscape, and Opera
- It is used to improve design, validate forms, detect browsers, and create cookies, among other tasks, in web pages

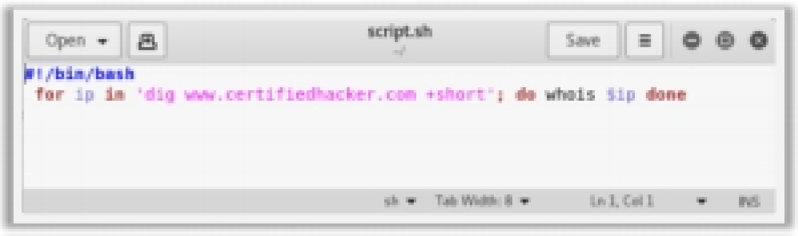
Advantages	Disadvantages
Less server interaction	Lacks in multithreading or multiprocessor capabilities
Immediate feedback for visitors	Cannot be used for networking applications
Increased interactivity	
Richer interfaces	

Bash Scripting

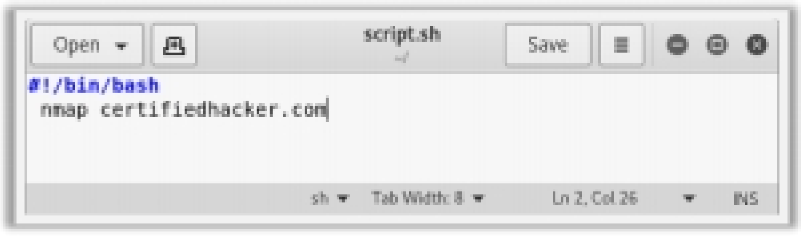
- Bash shell is a scripting environment that comes with Linux distro and is generally very useful for **automating certain actions** during penetration testing
- It is essential for the penetration tester to be familiar with the bash script environment to speed up their penetration testing work

Creating bash file

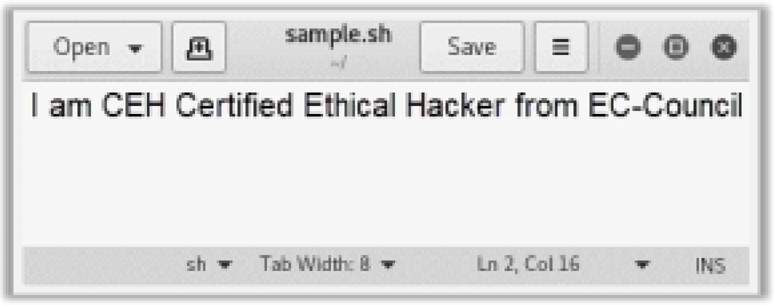
- Create a text file with any text editor and designate the .sh extension



```
#!/bin/bash
 for ip in 'dig www.certifiedhacker.com +short'; do whois $ip done
```

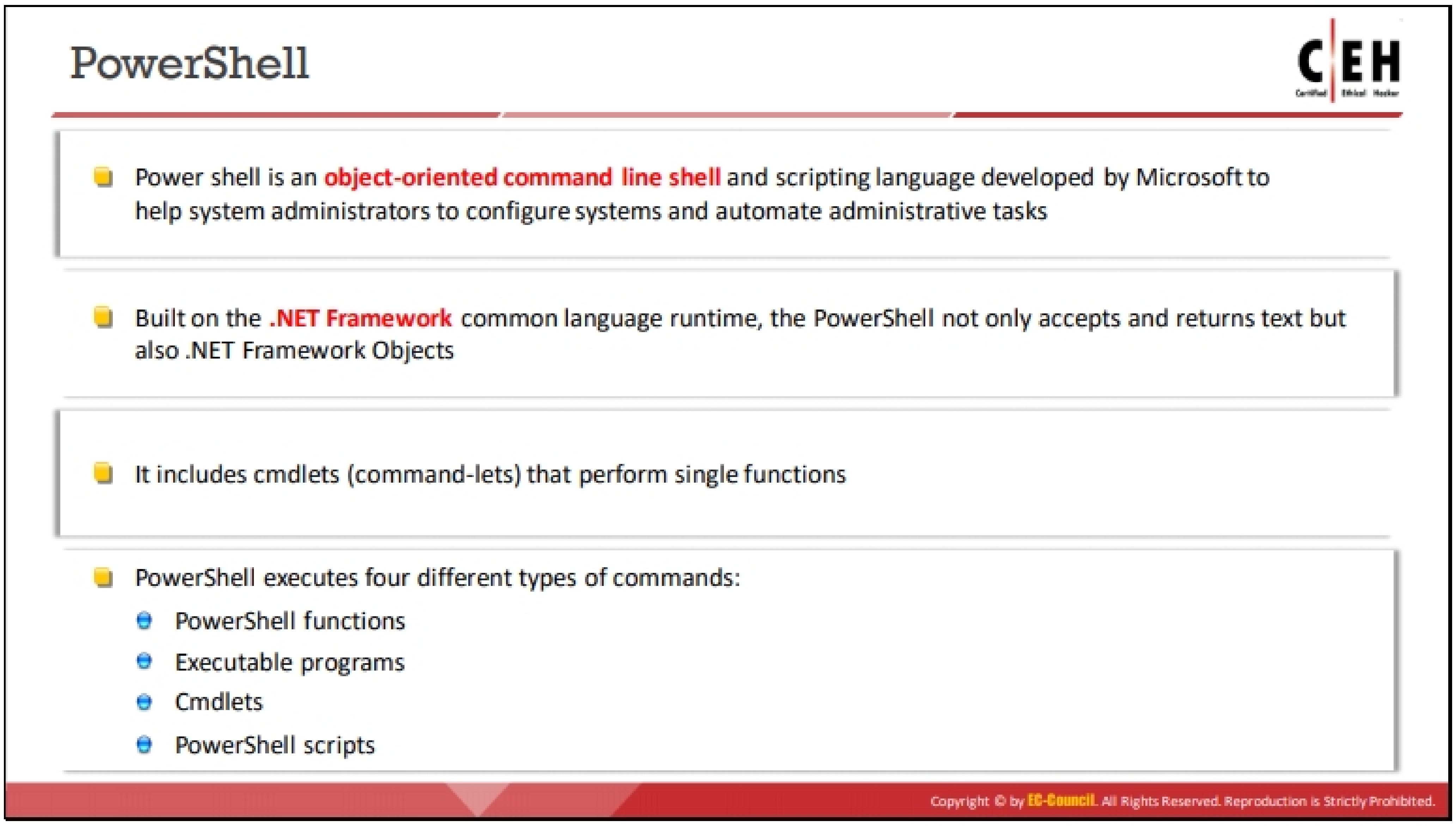


```
#!/bin/bash
 nmap certifiedhacker.com
```



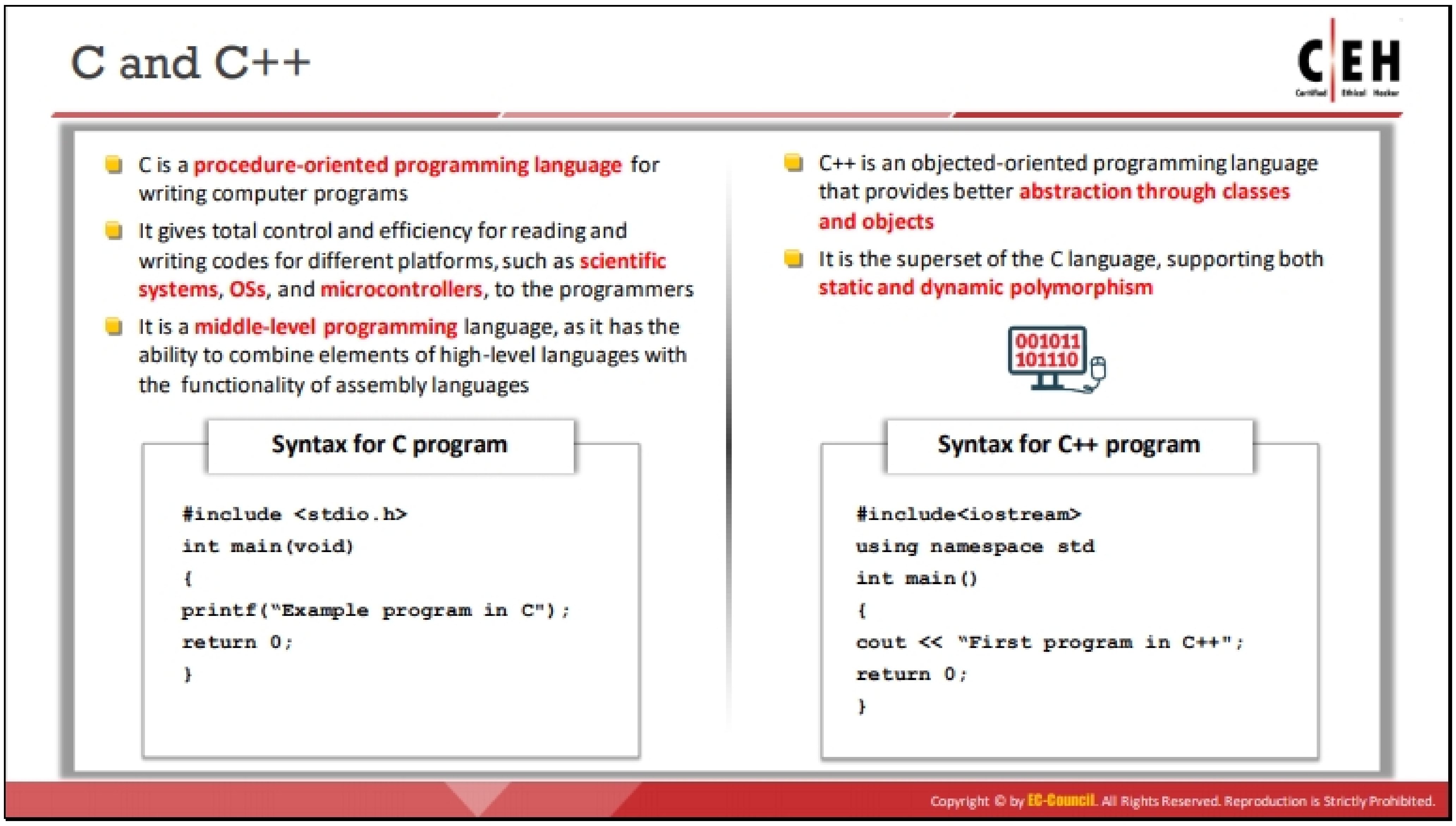
```
I am CEH Certified Ethical Hacker from EC-Council
```

Notes: ____



PowerShell

- Power shell is an **object-oriented command line shell** and scripting language developed by Microsoft to help system administrators to configure systems and automate administrative tasks
- Built on the **.NET Framework** common language runtime, the PowerShell not only accepts and returns text but also .NET Framework Objects
- It includes cmdlets (command-lets) that perform single functions
- PowerShell executes four different types of commands:
  - PowerShell functions
  - Executable programs
  - Cmdlets
  - PowerShell scripts



C and C++

- C is a **procedure-oriented programming language** for writing computer programs
- It gives total control and efficiency for reading and writing codes for different platforms, such as **scientific systems**, **OSs**, and **microcontrollers**, to the programmers
- It is a **middle-level programming** language, as it has the ability to combine elements of high-level languages with the functionality of assembly languages

Syntax for C program

```
#include <stdio.h>
int main(void)
{
printf(“Example program in C");
return 0;
}
```

- C++ is an objected-oriented programming language that provides better **abstraction through classes and objects**
- It is the superset of the C language, supporting both **static and dynamic polymorphism**

Syntax for C++ program

```
#include<iostream>
using namespace std
int main()
{
cout << “First program in C++";
return 0;
}
```

Notes:

C and C++ (Cont'd)

Key Features in C

- **Low level Features**: it is easy to write assembly codes in C, as it is closely related to low level language
- **Portability**: It can run on any compiler with little or no modification
- **Powerful**: Provides a wide variety of data types and functions and useful control and loop control statements
- **Bit Manipulation**: Provides a wide variety of bit manipulation operators
- **High Level Features**: More user friendly
- **Modular programming**: Code can be written in routines called functions that can be reused in other programs
- Supports efficient use of pointers, dynamic memory allocation, and graphic programming
- Has a rich set of library routines for string manipulations, I/O operations, mathematical functions, and other functions

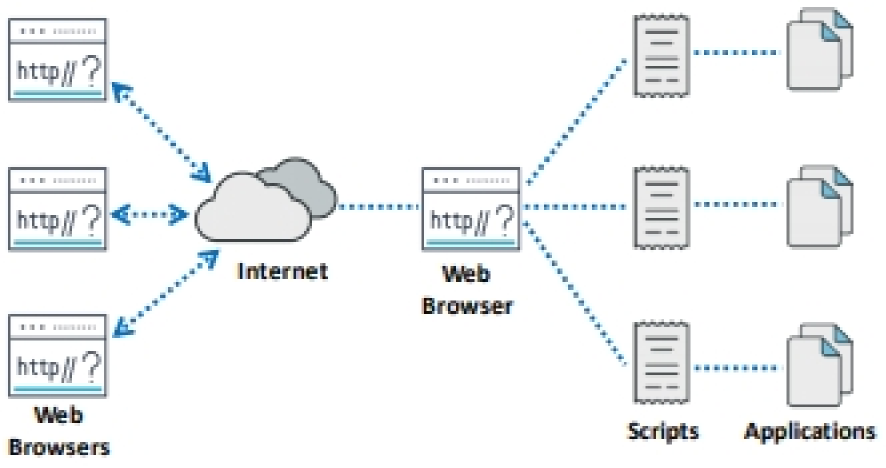
Key Features in C++

- **Classes**: Used to create user defined data types
- **Inheritance**: Allows one data type to acquire the properties of other data types
- **Data Abstraction**: Representative of key features without including background details
- **Encapsulation**: Wraps up of data in a single entity
- **Polymorphism**: Uses one interface for many implementations
- **Dynamic Binding**: Links a procedure call to code to be executed in response to the call
- **Message Passing**: A set of objects communicate through passing messages
- **Function Overloading**: A series of functions defined with different argument types that use the same function name
- **Operator Overloading**: Adds properties to operators for new data types
- **Other features include** try-catch-throw exception handling, stricter type checking, and more versatile access to data and functions

CGI

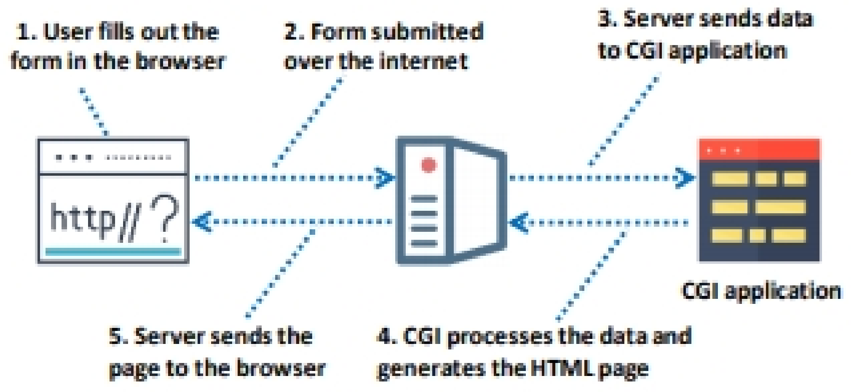
- Common Gateway Interface (CGI) is the standard way for a web server to connect to external applications

CGI based architecture


http:// ?
Internet
Web Browser
Scripts
Applications
Web Browsers

- CGI gathers information sent from a web browser to a web server, makes it available to an external program, and forwards the output received from program to the web browser

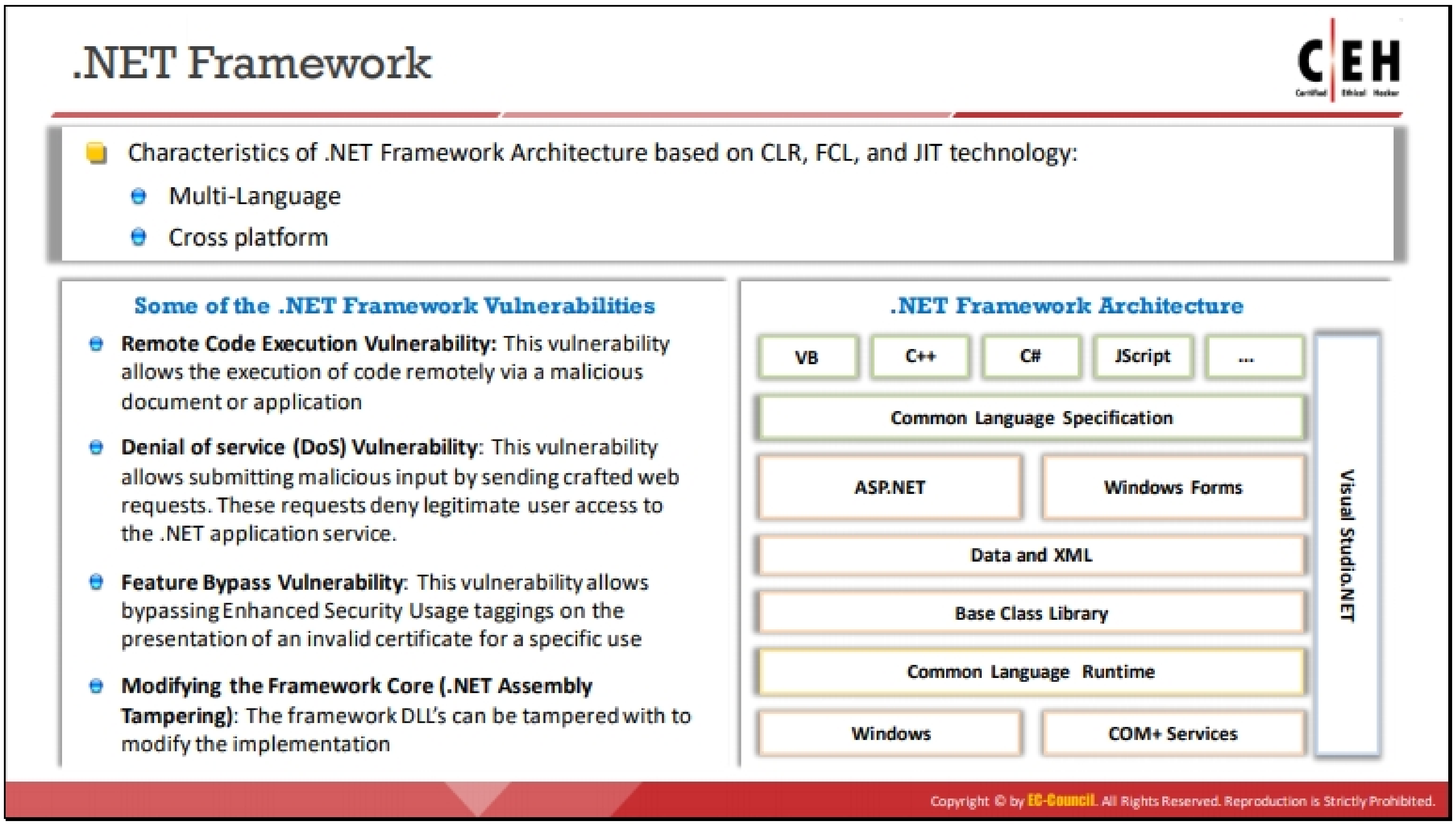
How a CGI request is processed?


1. User fills out the form in the browser
2. Form submitted over the internet
3. Server sends data to CGI application
http:// ?
CGI application
5. Server sends the page to the browser
4. CGI processes the data and generates the HTML page

- CGI is supported by many web servers and is language independent (widely used: Perl, C, and C++)

Notes: ____

Application Development Frameworks and Their Vulnerabilities



.NET Framework

- Characteristics of .NET Framework Architecture based on CLR, FCL, and JIT technology:
  - Multi-Language
  - Cross platform

Some of the .NET Framework Vulnerabilities

- **Remote Code Execution Vulnerability:** This vulnerability allows the execution of code remotely via a malicious document or application
- **Denial of service (DoS) Vulnerability**: This vulnerability allows submitting malicious input by sending crafted web requests. These requests deny legitimate user access to the .NET application service.
- **Feature Bypass Vulnerability**: This vulnerability allows bypassing Enhanced Security Usage taggings on the presentation of an invalid certificate for a specific use
- **Modifying the Framework Core (.NET Assembly Tampering)**: The framework DLL's can be tampered with to modify the implementation

.NET Framework Architecture

VB | C++ | C# | JScript | ...
Common Language Specification
ASP.NET | Windows Forms
Data and XML
Base Class Library
Common Language Runtime
Windows | COM+ Services
Visual Studio.NET

Notes: ____

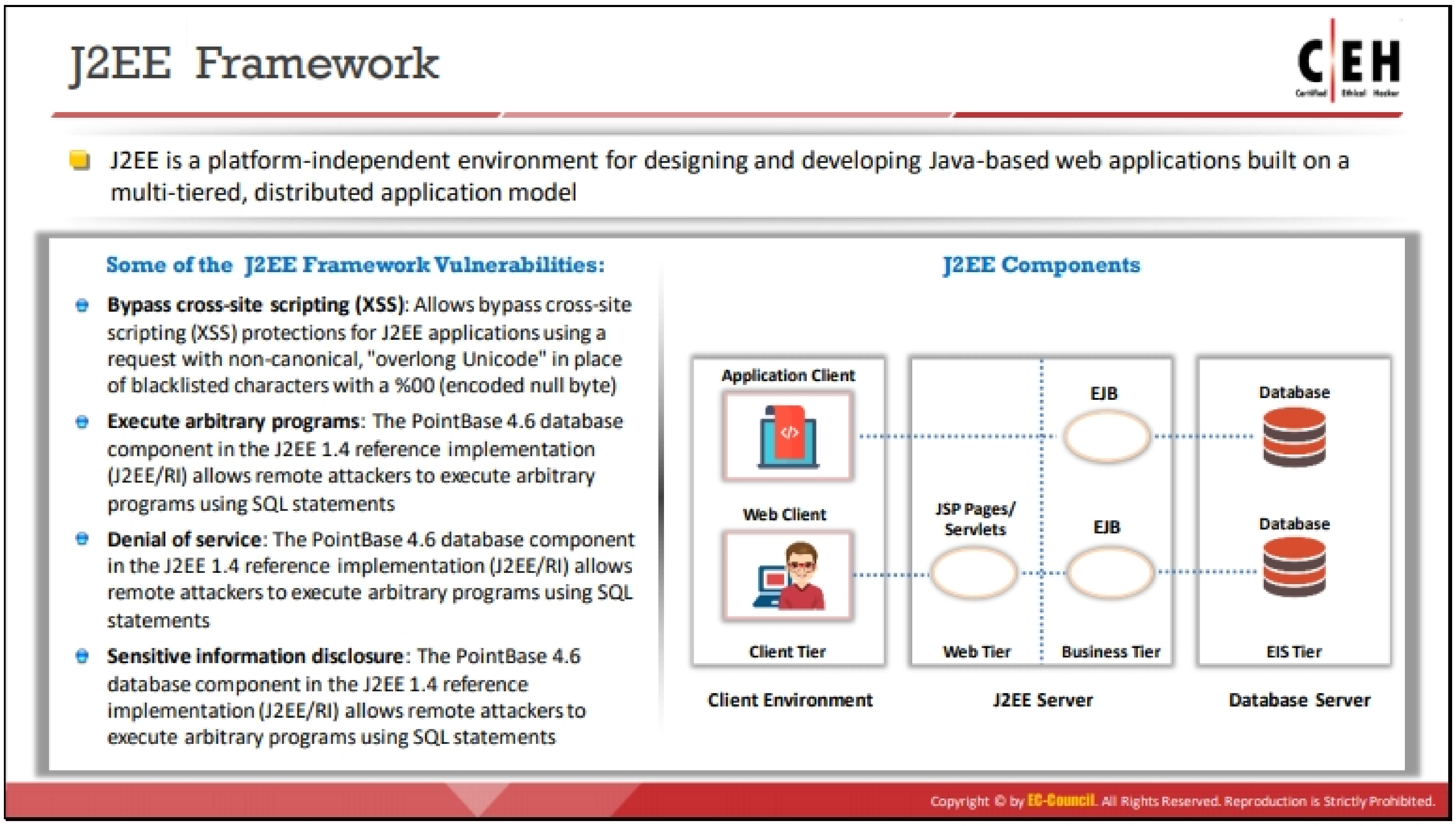
____

____

____

____

____



J2EE Framework

- J2EE is a platform-independent environment for designing and developing Java-based web applications built on a multi-tiered, distributed application model

Some of the J2EE Framework Vulnerabilities:

- **Bypass cross-site scripting (XSS)**: Allows bypass cross-site scripting (XSS) protections for J2EE applications using a request with non-canonical, "overlong Unicode" in place of blacklisted characters with a %00 (encoded null byte)
- **Execute arbitrary programs**: The PointBase 4.6 database component in the J2EE 1.4 reference implementation (J2EE/RI) allows remote attackers to execute arbitrary programs using SQL statements
- **Denial of service**: The PointBase 4.6 database component in the J2EE 1.4 reference implementation (J2EE/RI) allows remote attackers to execute arbitrary programs using SQL statements
- **Sensitive information disclosure**: The PointBase 4.6 database component in the J2EE 1.4 reference implementation (J2EE/RI) allows remote attackers to execute arbitrary programs using SQL statements

J2EE Components

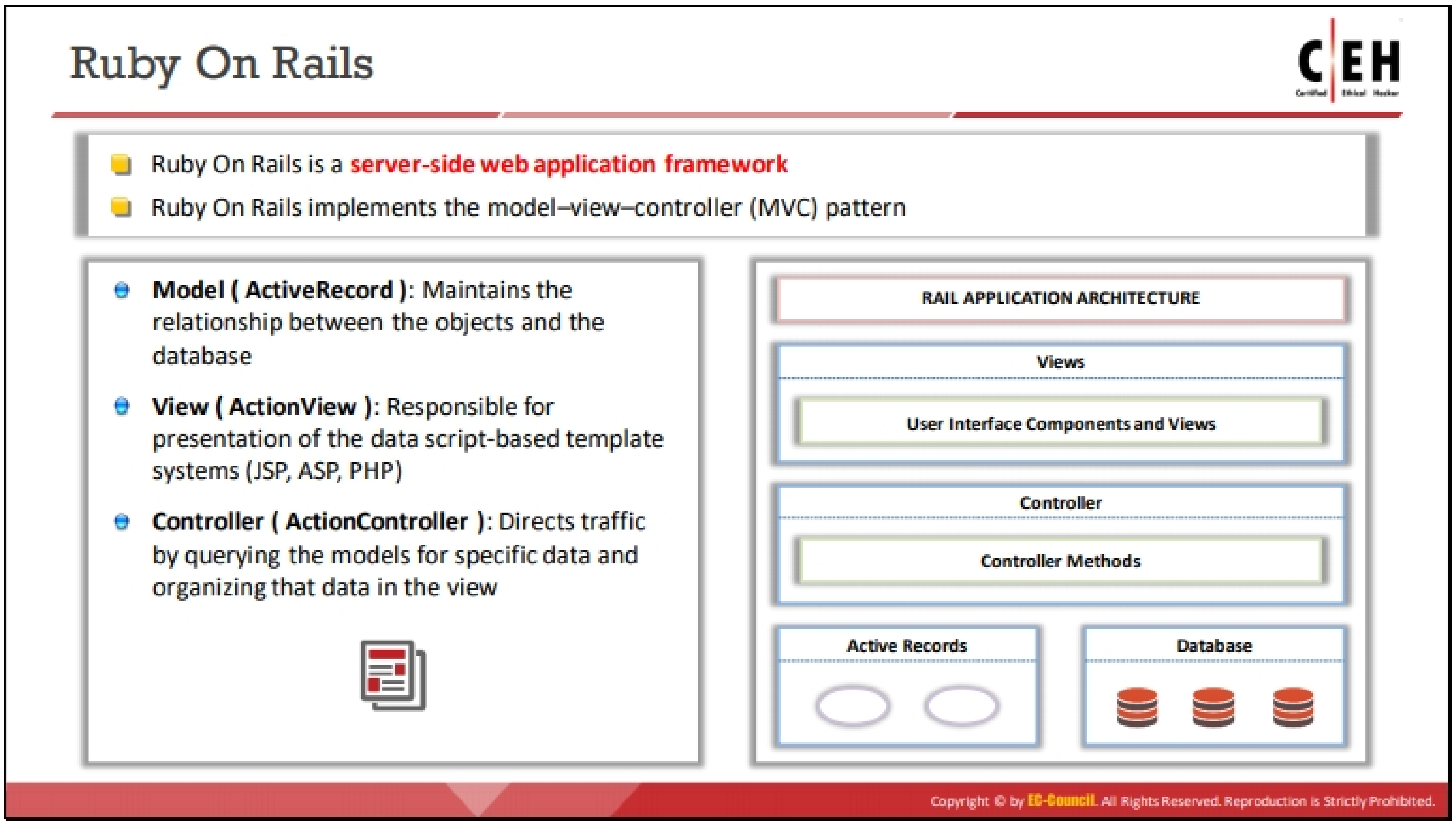
ColdFusion

- ColdFusion is a rapid **web application development platform**
- The ColdFusion platform is built on Java and uses the Apache Tomcat J2EE container

Some of the ColdFusion Framework Vulnerabilities:

- **Directory Traversal**
- **Unvalidated Browser Input**
- **ColdFusion CSRF Vulnerability**
- **CFFILE, CFFTP, and CFPOP Vulnerability**
- **ColdFusion DoS Attack Vulnerability**

Notes: ____



Ruby On Rails

- Ruby On Rails is a **server-side web application framework**
- Ruby On Rails implements the model–view–controller (MVC) pattern

- **Model (ActiveRecord)**: Maintains the relationship between the objects and the database
- **View (ActionView)**: Responsible for presentation of the data script-based template systems (JSP, ASP, PHP)
- **Controller (ActionController)**: Directs traffic by querying the models for specific data and organizing that data in the view

RAIL APPLICATION ARCHITECTURE

Views

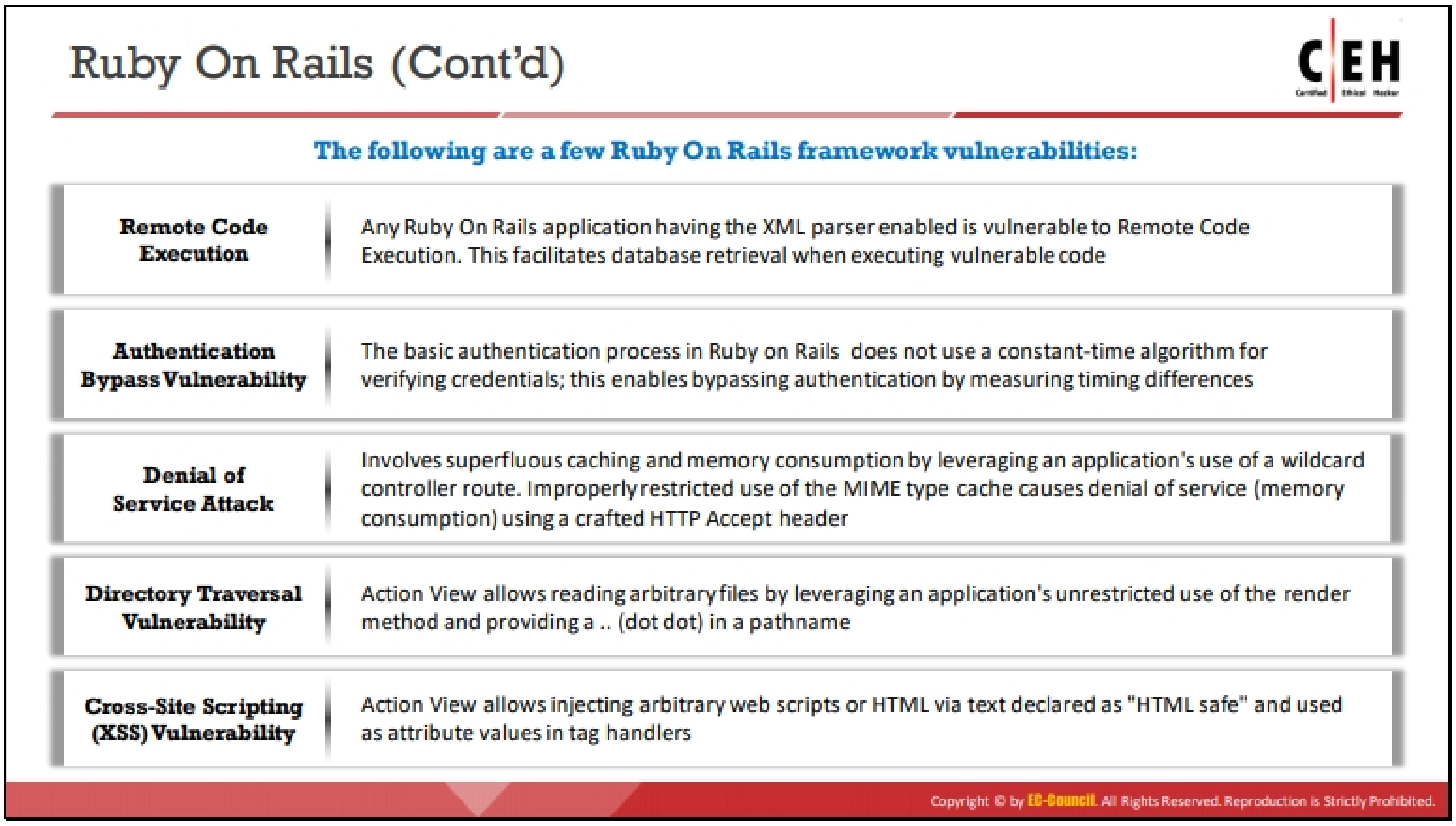
User Interface Components and Views

Controller

Controller Methods

Active Records

Database

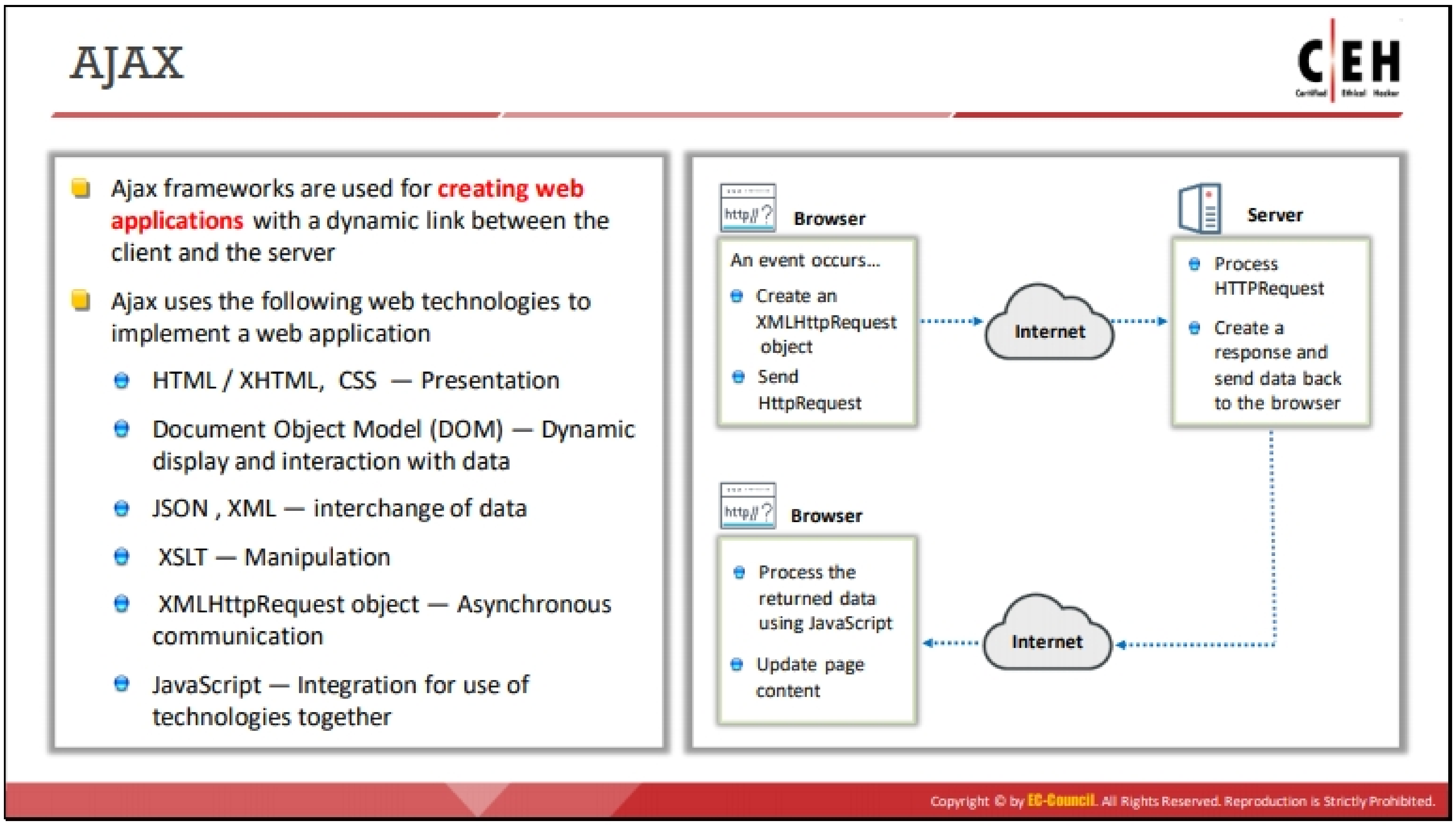


Ruby On Rails (Cont'd)

The following are a few Ruby On Rails framework vulnerabilities:

Remote Code Execution	Any Ruby On Rails application having the XML parser enabled is vulnerable to Remote Code Execution. This facilitates database retrieval when executing vulnerable code
Authentication Bypass Vulnerability	The basic authentication process in Ruby on Rails does not use a constant-time algorithm for verifying credentials; this enables bypassing authentication by measuring timing differences
Denial of Service Attack	Involves superfluous caching and memory consumption by leveraging an application's use of a wildcard controller route. Improperly restricted use of the MIME type cache causes denial of service (memory consumption) using a crafted HTTP Accept header
Directory Traversal Vulnerability	Action View allows reading arbitrary files by leveraging an application's unrestricted use of the render method and providing a .. (dot dot) in a pathname
Cross-Site Scripting (XSS) Vulnerability	Action View allows injecting arbitrary web scripts or HTML via text declared as "HTML safe" and used as attribute values in tag handlers

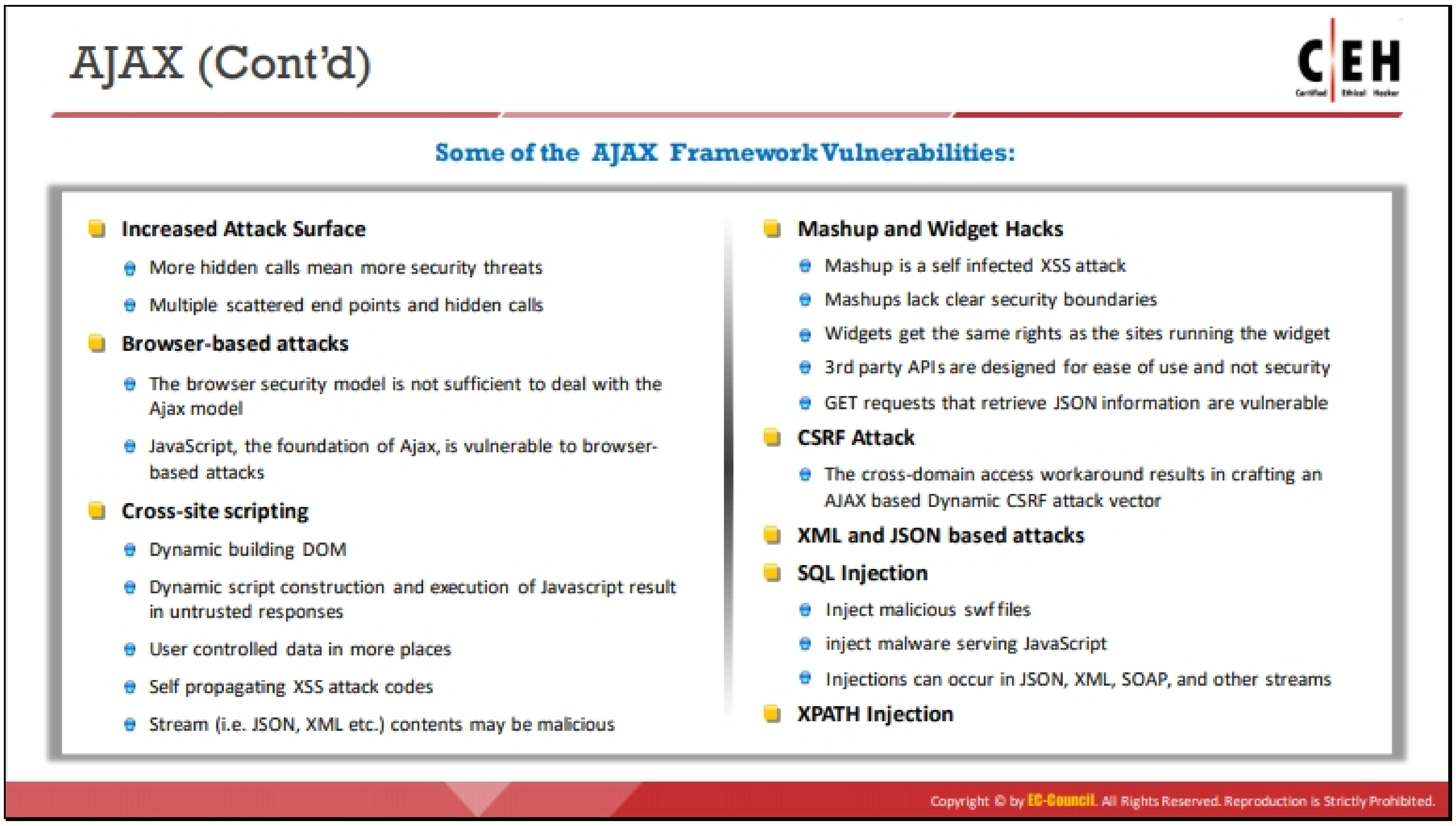
Notes:



AJAX

- Ajax frameworks are used for **creating web applications** with a dynamic link between the client and the server
- Ajax uses the following web technologies to implement a web application
  - HTML / XHTML, CSS — Presentation
  - Document Object Model (DOM) — Dynamic display and interaction with data
  - JSON , XML — interchange of data
  - XSLT — Manipulation
  - XMLHttpRequest object — Asynchronous communication
  - JavaScript — Integration for use of technologies together

Browser
An event occurs...
Create an XMLHttpRequest object
Send HttpRequest
Internet
Server
Process HTTPRequest
Create a response and send data back to the browser
Browser
Process the returned data using JavaScript
Update page content
Internet



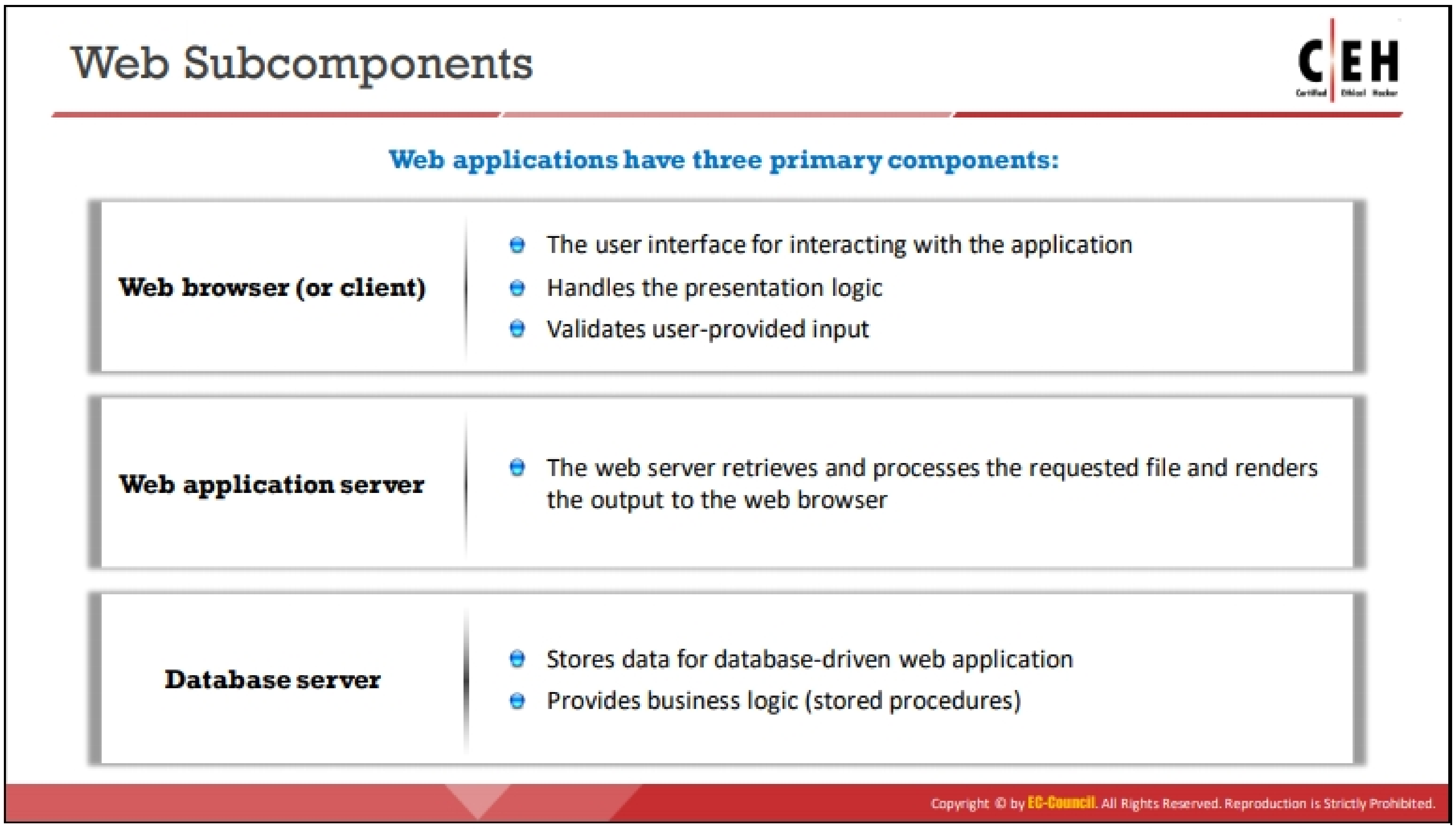
AJAX (Cont'd)

Some of the AJAX Framework Vulnerabilities:

- **Increased Attack Surface**
  - More hidden calls mean more security threats
  - Multiple scattered end points and hidden calls
- **Browser-based attacks**
  - The browser security model is not sufficient to deal with the Ajax model
  - JavaScript, the foundation of Ajax, is vulnerable to browser-based attacks
- **Cross-site scripting**
  - Dynamic building DOM
  - Dynamic script construction and execution of Javascript result in untrusted responses
  - User controlled data in more places
  - Self propagating XSS attack codes
  - Stream (i.e. JSON, XML etc.) contents may be malicious
- **Mashup and Widget Hacks**
  - Mashup is a self infected XSS attack
  - Mashups lack clear security boundaries
  - Widgets get the same rights as the sites running the widget
  - 3rd party APIs are designed for ease of use and not security
  - GET requests that retrieve JSON information are vulnerable
- **CSRF Attack**
  - The cross-domain access workaround results in crafting an AJAX based Dynamic CSRF attack vector
- **XML and JSON based attacks**
- **SQL Injection**
  - Inject malicious swf files
  - inject malware serving JavaScript
  - Injections can occur in JSON, XML, SOAP, and other streams
- **XPATH Injection**

Notes: ____________________

Web Subcomponents



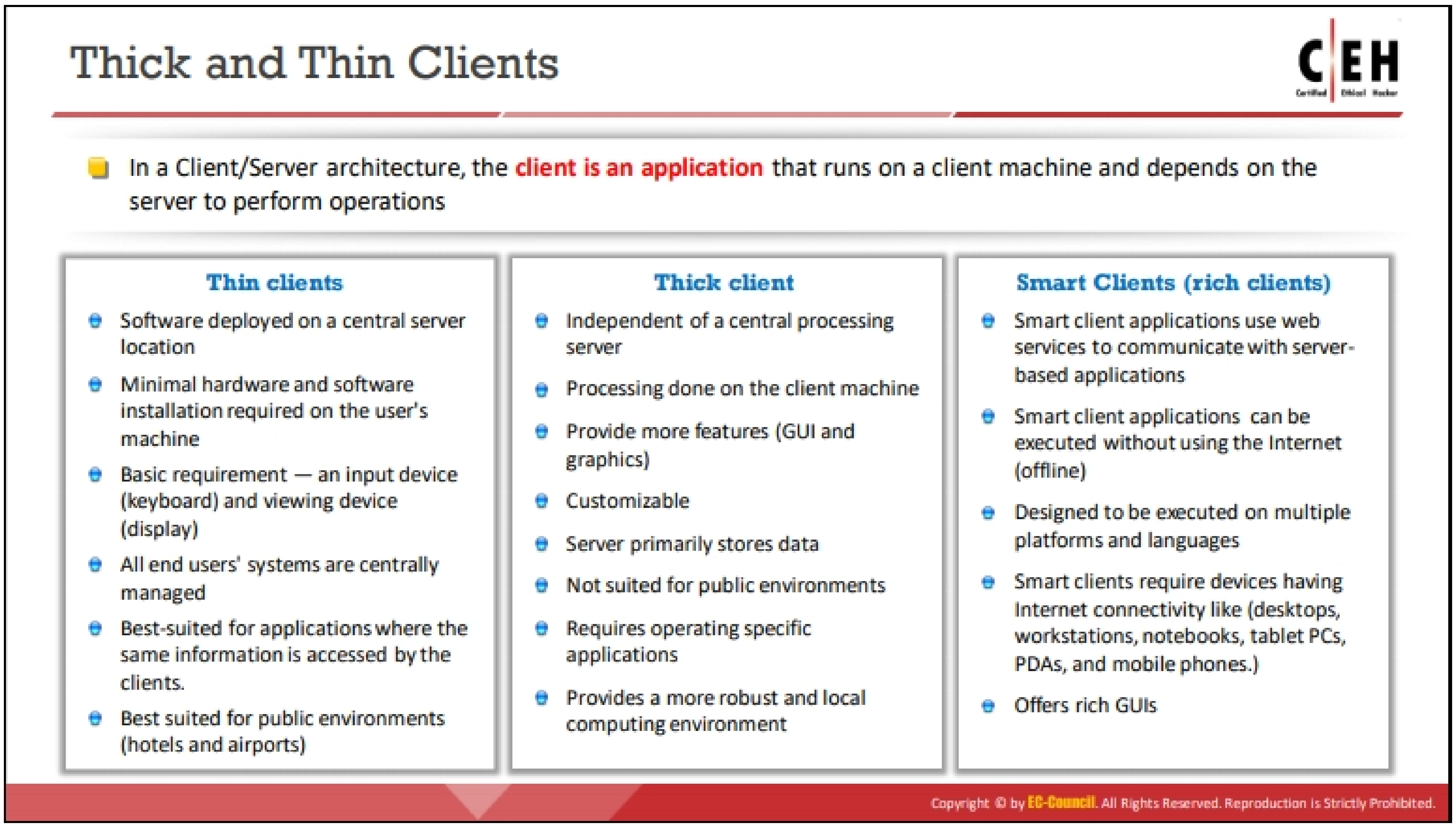
Web Subcomponents

CEH
Certified Ethical Hacker

Web applications have three primary components:

Web browser (or client)	The user interface for interacting with the application Handles the presentation logic Validates user-provided input
Web application server	The web server retrieves and processes the requested file and renders the output to the web browser
Database server	Stores data for database-driven web application Provides business logic (stored procedures)

Notes: ____



Thick and Thin Clients

- In a Client/Server architecture, the client is an application that runs on a client machine and depends on the server to perform operations

Thin clients

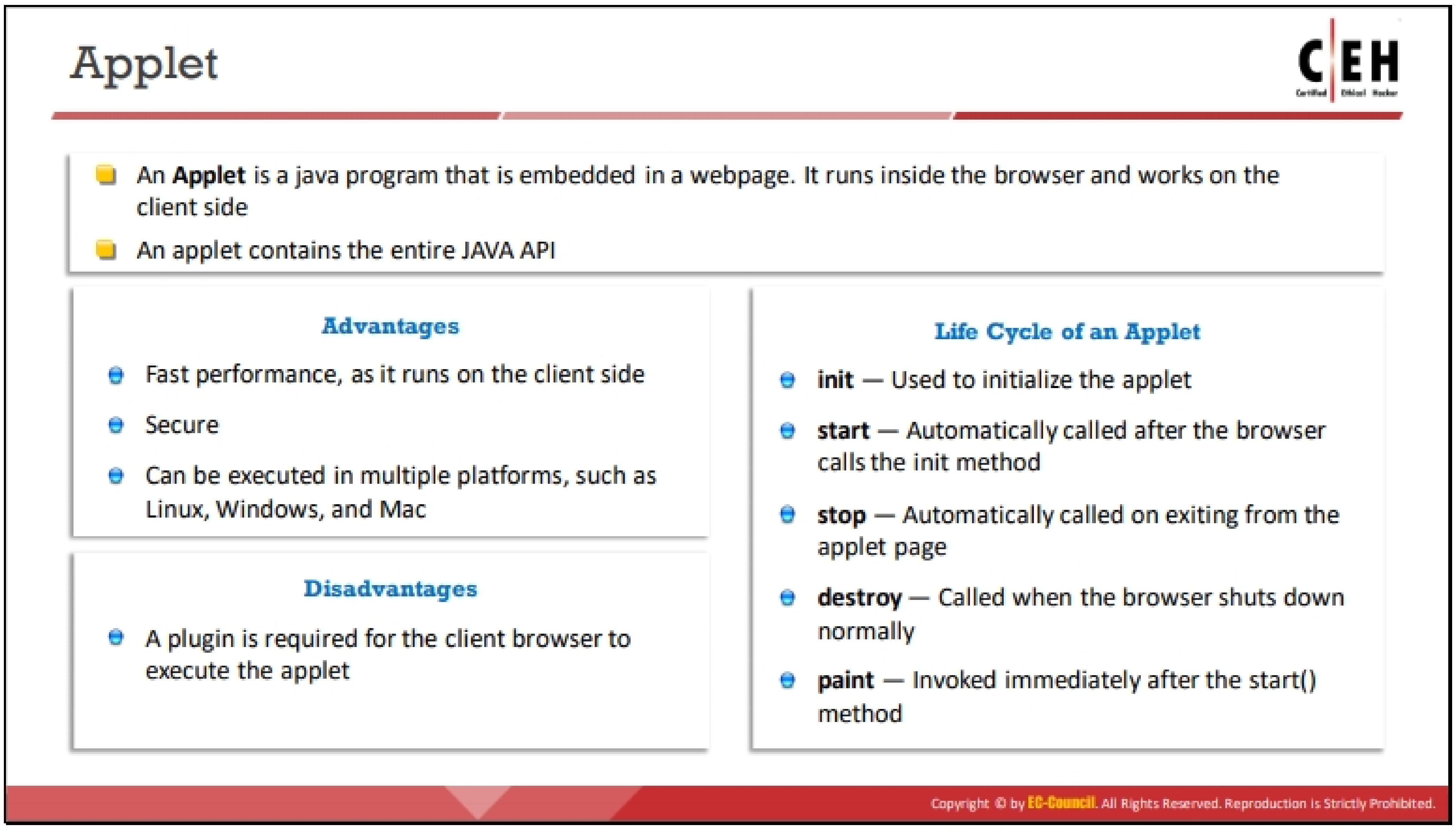
- Software deployed on a central server location
- Minimal hardware and software installation required on the user's machine
- Basic requirement — an input device (keyboard) and viewing device (display)
- All end users' systems are centrally managed
- Best-suited for applications where the same information is accessed by the clients.
- Best suited for public environments (hotels and airports)

Thick client

- Independent of a central processing server
- Processing done on the client machine
- Provide more features (GUI and graphics)
- Customizable
- Server primarily stores data
- Not suited for public environments
- Requires operating specific applications
- Provides a more robust and local computing environment

Smart Clients (rich clients)

- Smart client applications use web services to communicate with server-based applications
- Smart client applications can be executed without using the Internet (offline)
- Designed to be executed on multiple platforms and languages
- Smart clients require devices having Internet connectivity like (desktops, workstations, notebooks, tablet PCs, PDAs, and mobile phones.)
- Offers rich GUIs



Applet

- An **Applet** is a java program that is embedded in a webpage. It runs inside the browser and works on the client side
- An applet contains the entire JAVA API

Advantages

- Fast performance, as it runs on the client side
- Secure
- Can be executed in multiple platforms, such as Linux, Windows, and Mac

Disadvantages

- A plugin is required for the client browser to execute the applet

Life Cycle of an Applet

- **init** — Used to initialize the applet
- **start** — Automatically called after the browser calls the init method
- **stop** — Automatically called on exiting from the applet page
- **destroy** — Called when the browser shuts down normally
- **paint** — Invoked immediately after the start() method

Notes: ____

____

____

____

____

____

Servlet

- A servlet is a Java program deployed on the server that responds to client requests and dynamically generates responses
- Servlets are robust and scalable

Advantages

- Allows the creation of a dynamic web page
- Inherits all features of JAVA
- Portable across web servers
- Enables servlet and server communication

Disadvantages

- Designing in servlet is difficult
- Performance reduced when an application implements servlets
- Difficult to build complex business logic
- Requires the Java Runtime Environment on the server to executing servlets

Life Cycle of a Servlet

- **init()** - Initialize the servlet instance
- **service()** - Invoked after every service request
- **destroy()** - Remove the servlet out of service

ActiveX

- **ActiveX** is a set of technologies and services based on the Component Object Model (COM), which makes it easy to integrate and reuse any component
- Brings component-based development to the Internet
- COM/DCOM Lets ActiveX components run anywhere

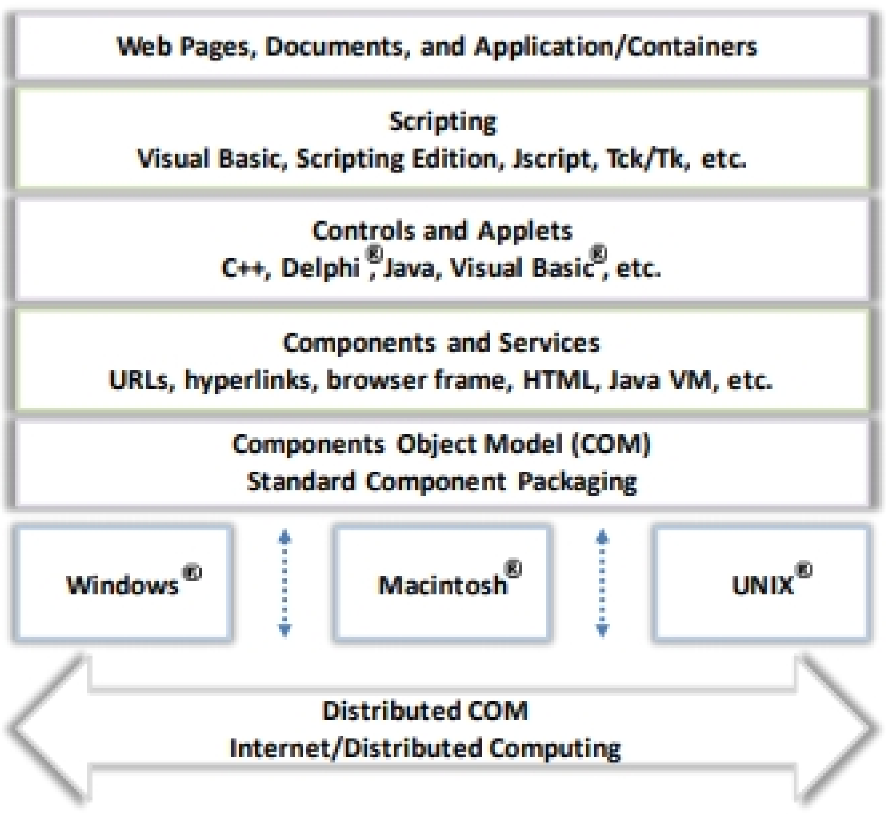
ActiveX Controls

- Controls that can be manipulated visually by GUI tools
- Java VM and Java Component are ActiveX Components

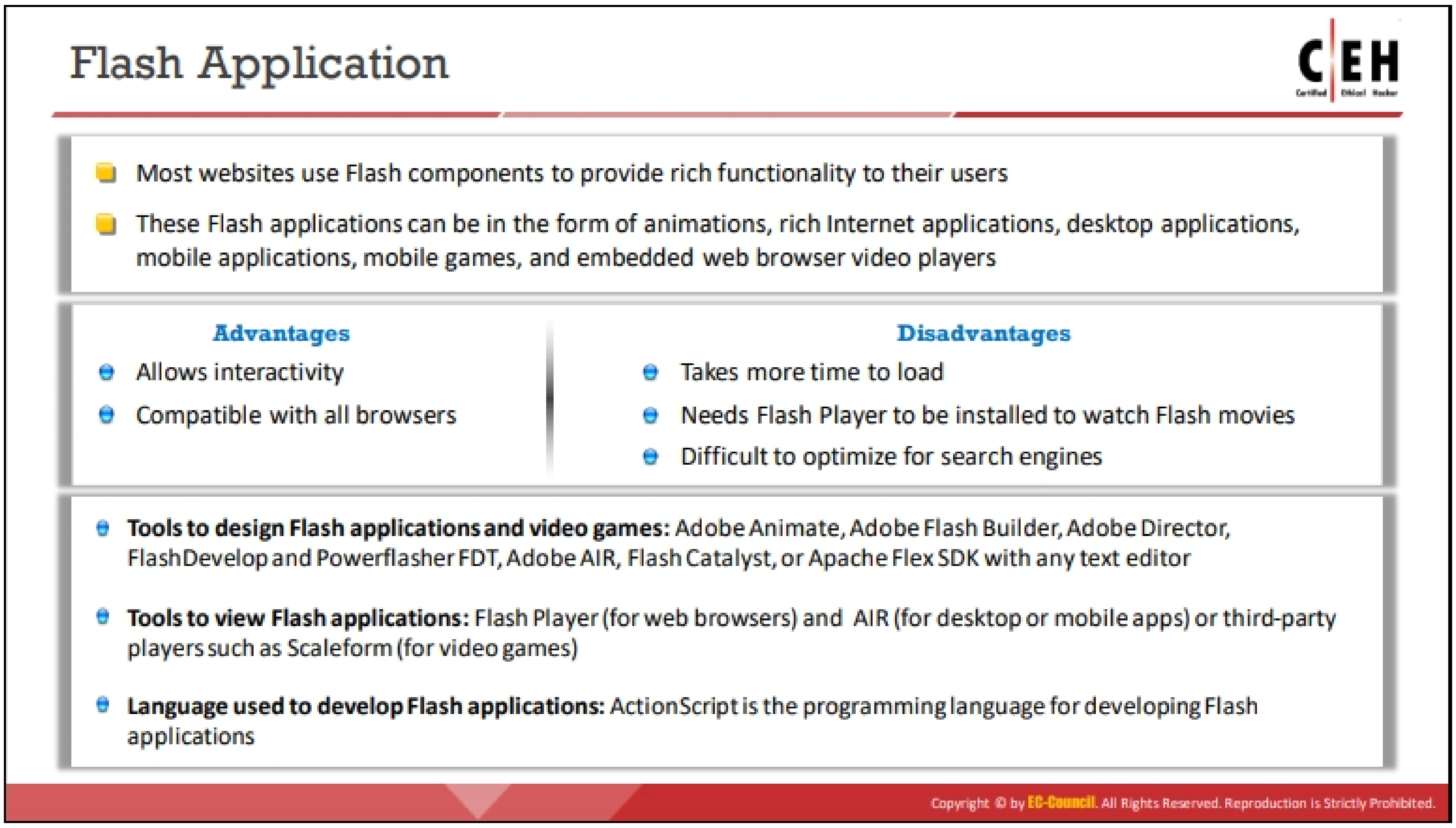
ActiveX Scripting

- Supports any scripting language, such as VBScript, JScript, Perl, PowerScript, and Tck/Tk

Elements of ActiveX


Web Pages, Documents, and Application/Containers
Scripting
Visual Basic, Scripting Edition, Jscript, Tck/Tk, etc.
Controls and Applets
C++, Delphi®, Java, Visual Basic®, etc.
Components and Services
URLs, hyperlinks, browser frame, HTML, Java VM, etc.
Components Object Model (COM)
Standard Component Packaging
Windows®
Macintosh®
UNIX®
Distributed COM
Internet/Distributed Computing

Notes: ____________________



Flash Application

- Most websites use Flash components to provide rich functionality to their users
- These Flash applications can be in the form of animations, rich Internet applications, desktop applications, mobile applications, mobile games, and embedded web browser video players

Advantages	Disadvantages
Allows interactivity	Takes more time to load
Compatible with all browsers	Needs Flash Player to be installed to watch Flash movies
	Difficult to optimize for search engines

- **Tools to design Flash applications and video games:** Adobe Animate, Adobe Flash Builder, Adobe Director, FlashDevelop and Powerflasher FDT, Adobe AIR, Flash Catalyst, or Apache Flex SDK with any text editor
- **Tools to view Flash applications:** Flash Player (for web browsers) and AIR (for desktop or mobile apps) or third-party players such as Scaleform (for video games)
- **Language used to develop Flash applications:** ActionScript is the programming language for developing Flash applications

Database Connectivity

Notes: ____

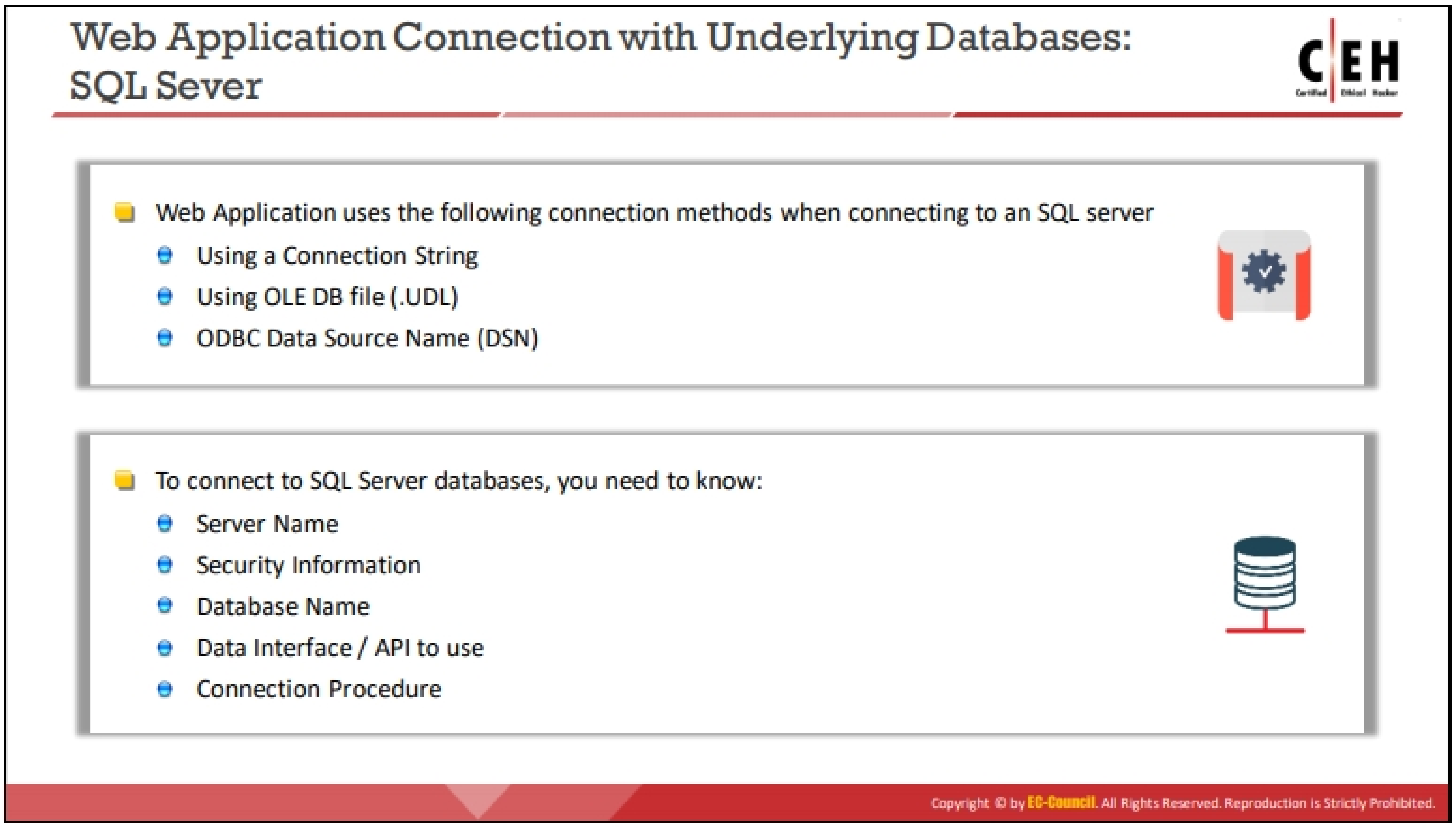
____

____

____

____

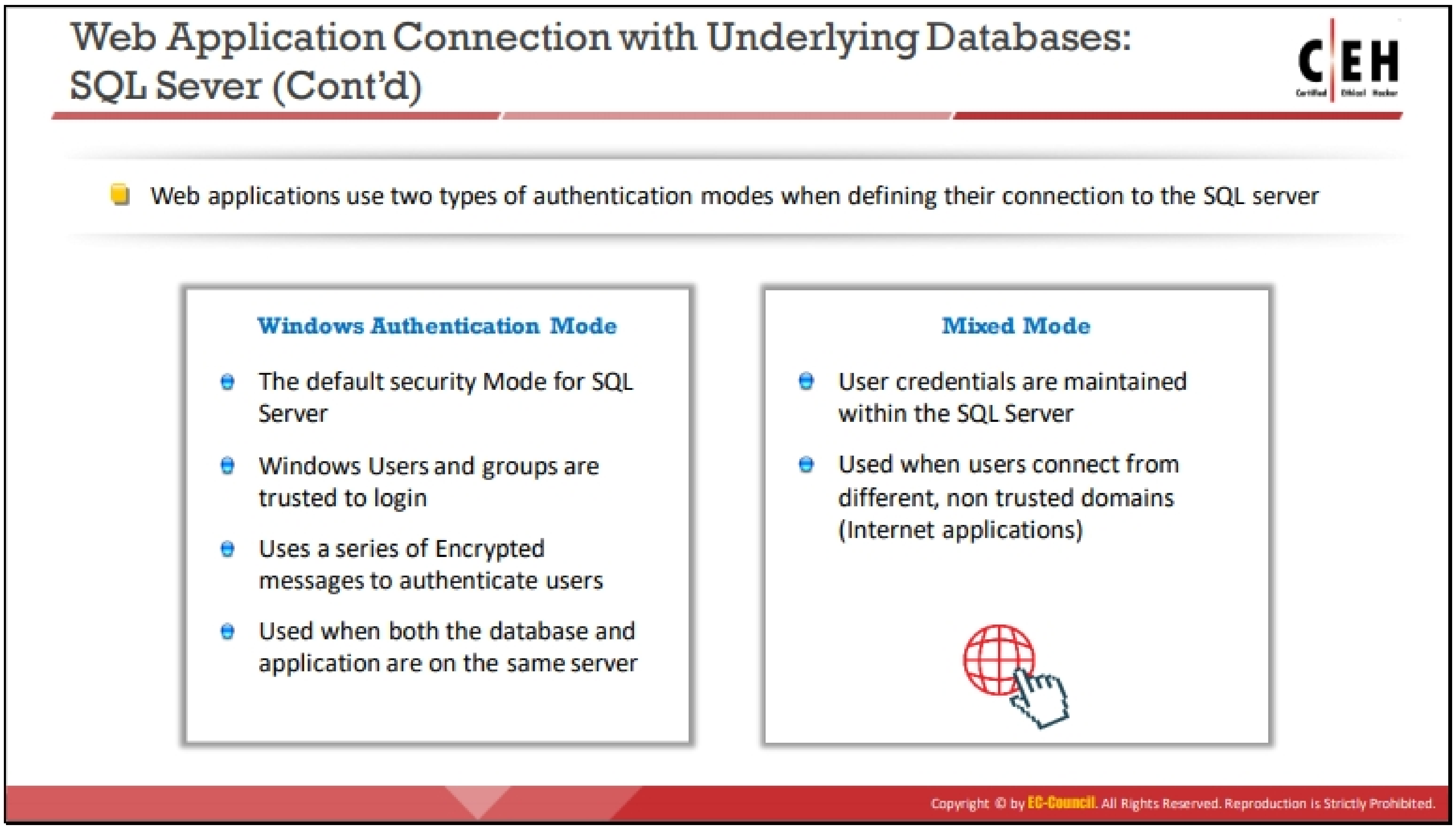
____



Web Application Connection with Underlying Databases: SQL Sever

- Web Application uses the following connection methods when connecting to an SQL server
  - Using a Connection String
  - Using OLE DB file (.UDL)
  - ODBC Data Source Name (DSN)

- To connect to SQL Server databases, you need to know:
  - Server Name
  - Security Information
  - Database Name
  - Data Interface / API to use
  - Connection Procedure



Web Application Connection with Underlying Databases: SQL Sever (Cont'd)

- Web applications use two types of authentication modes when defining their connection to the SQL server

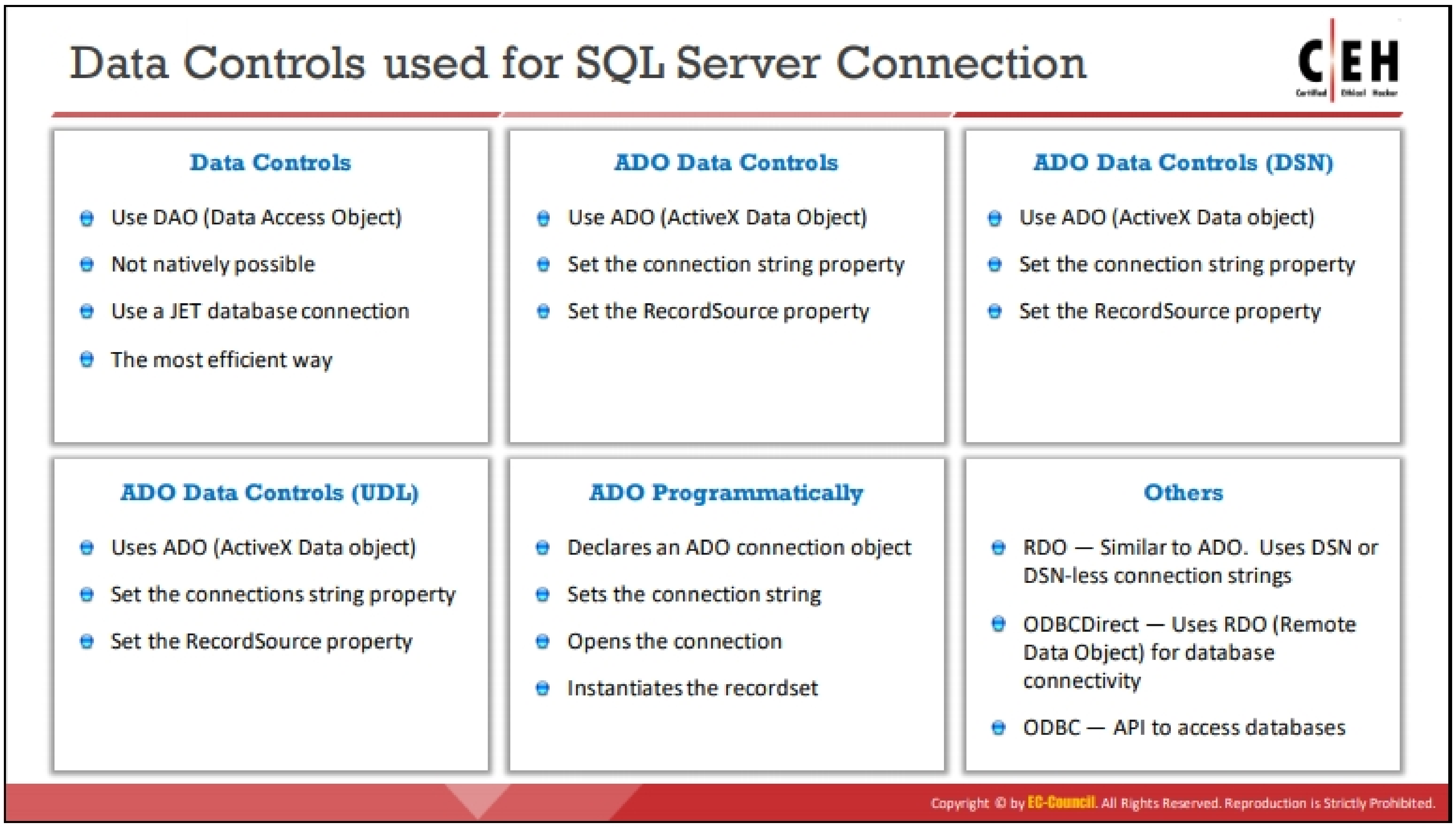
Windows Authentication Mode

- The default security Mode for SQL Server
- Windows Users and groups are trusted to login
- Uses a series of Encrypted messages to authenticate users
- Used when both the database and application are on the same server

Mixed Mode

- User credentials are maintained within the SQL Server
- Used when users connect from different, non trusted domains (Internet applications)

Notes:



Data Controls used for SQL Server Connection

Data Controls

- Use DAO (Data Access Object)
- Not natively possible
- Use a JET database connection
- The most efficient way

ADO Data Controls

- Use ADO (ActiveX Data Object)
- Set the connection string property
- Set the RecordSource property

ADO Data Controls (DSN)

- Use ADO (ActiveX Data object)
- Set the connection string property
- Set the RecordSource property

ADO Data Controls (UDL)

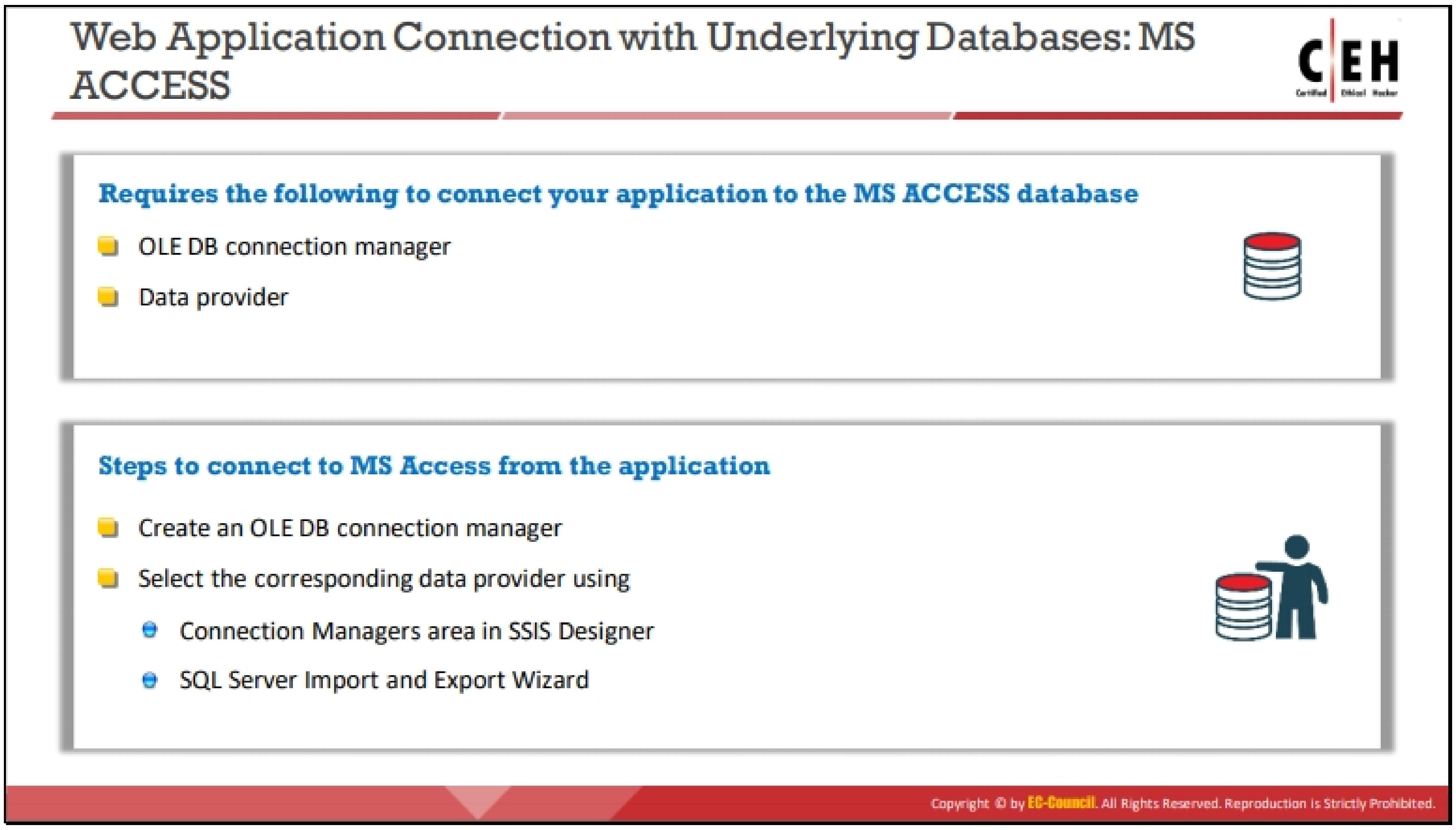
- Uses ADO (ActiveX Data object)
- Set the connections string property
- Set the RecordSource property

ADO Programmatically

- Declares an ADO connection object
- Sets the connection string
- Opens the connection
- Instantiates the recordset

Others

- RDO — Similar to ADO. Uses DSN or DSN-less connection strings
- ODBCDirect — Uses RDO (Remote Data Object) for database connectivity
- ODBC — API to access databases



Web Application Connection with Underlying Databases: MS ACCESS

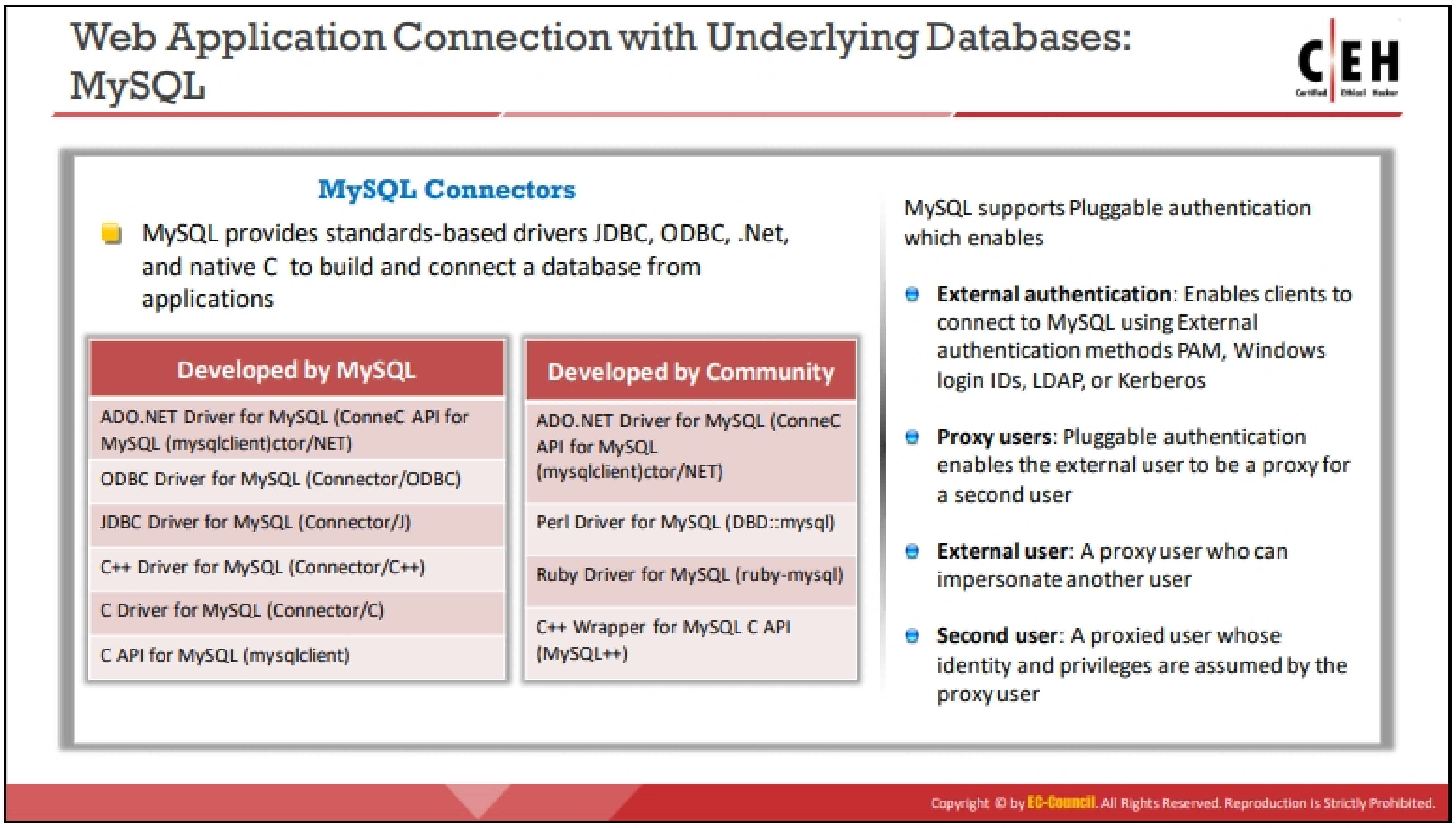
Requires the following to connect your application to the MS ACCESS database

- OLE DB connection manager
- Data provider

Steps to connect to MS Access from the application

- Create an OLE DB connection manager
- Select the corresponding data provider using
  - Connection Managers area in SSIS Designer
  - SQL Server Import and Export Wizard

Notes: ____



Web Application Connection with Underlying Databases: MySQL

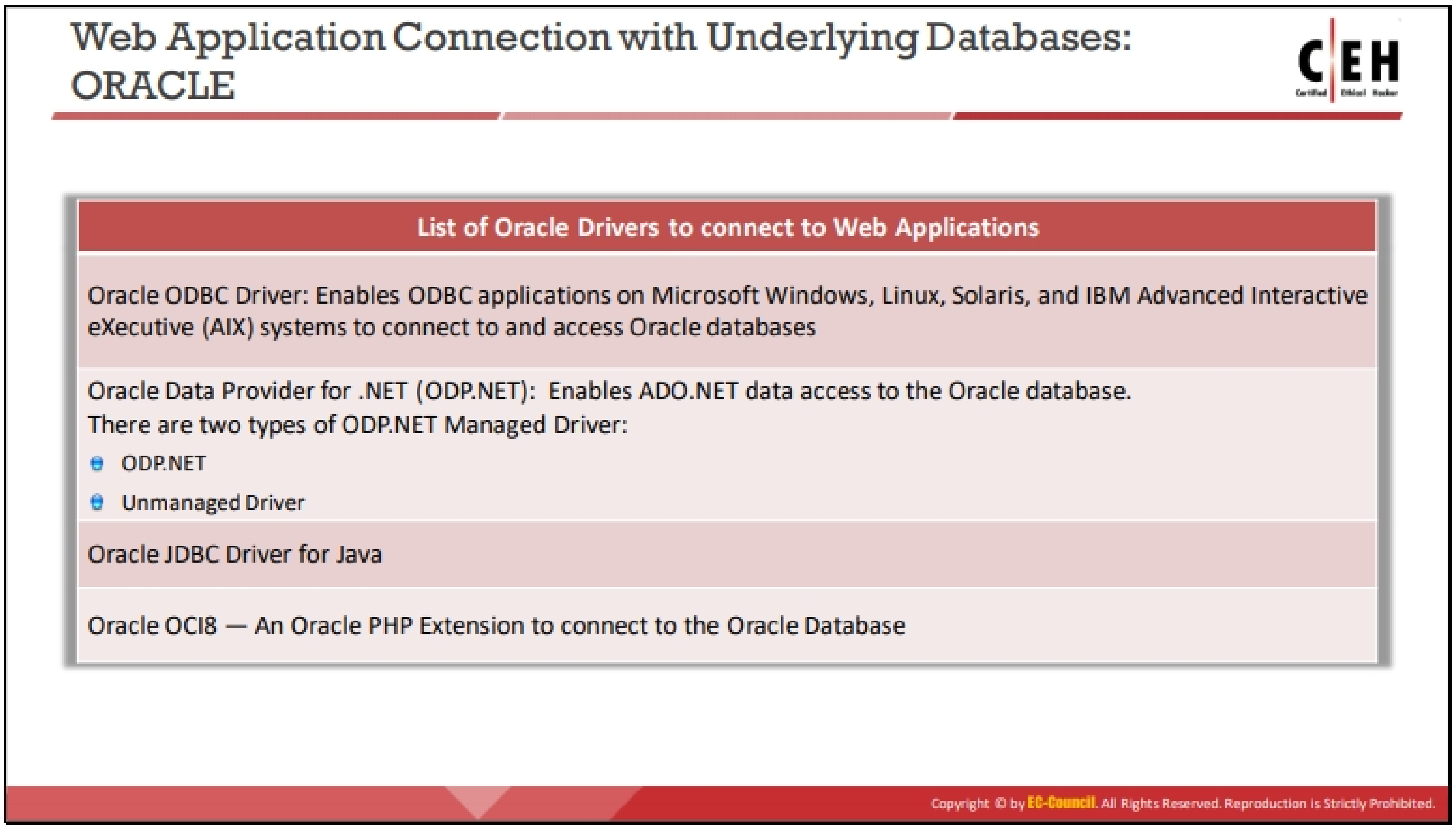
MySQL Connectors

- MySQL provides standards-based drivers JDBC, ODBC, .Net, and native C to build and connect a database from applications

Developed by MySQL	Developed by Community
ADO.NET Driver for MySQL (ConneC API for MySQL (mysqlclient)ctor/NET)	ADO.NET Driver for MySQL (ConneC API for MySQL (mysqlclient)ctor/NET)
ODBC Driver for MySQL (Connector/ODBC)	Perl Driver for MySQL (DBD::mysql)
JDBC Driver for MySQL (Connector/J)	Ruby Driver for MySQL (ruby-mysql)
C++ Driver for MySQL (Connector/C++)	C++ Wrapper for MySQL C API (MySQL++)
C Driver for MySQL (Connector/C)	
C API for MySQL (mysqlclient)	

MySQL supports Pluggable authentication which enables

- **External authentication**: Enables clients to connect to MySQL using External authentication methods PAM, Windows login IDs, LDAP, or Kerberos
- **Proxy users**: Pluggable authentication enables the external user to be a proxy for a second user
- **External user**: A proxy user who can impersonate another user
- **Second user**: A proxied user whose identity and privileges are assumed by the proxy user



Web Application Connection with Underlying Databases: ORACLE

List of Oracle Drivers to connect to Web Applications
Oracle ODBC Driver: Enables ODBC applications on Microsoft Windows, Linux, Solaris, and IBM Advanced Interactive eXecutive (AIX) systems to connect to and access Oracle databases
Oracle Data Provider for .NET (ODP.NET): Enables ADO.NET data access to the Oracle database. There are two types of ODP.NET Managed Driver: • ODP.NET • Unmanaged Driver
Oracle JDBC Driver for Java
Oracle OCI8 — An Oracle PHP Extension to connect to the Oracle Database

Notes: ____

____

____

____

____

____